symantec™

Norton SystemWorks™ 2004 Professional

User's Guide

Norton SystemWorks™ Professional User’s Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 7.0

PN: 10109296

Copyright Notice

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Symantec, the Symantec logo, Norton SystemWorks, Norton Password Manager, Norton SystemWorks Professional, LiveUpdate, Norton AntiVirus, Norton Utilities, Norton CleanSweep, Norton GoBack, and Norton Ghost are U.S. registered trademarks of Symantec Corporation. Rescue Disk and Symantec AntiVirus are trademarks of Symantec Corporation.

Process Viewer developed 1995-2003 by Igor Nys. Passmark PerformanceTest is copyright by PassMark Software.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT
Norton SystemWorks Pro

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "I ACCEPT THE LICENSE AGREEMENT" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT ACCEPT THE LICENSE AGREEMENT" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE AND CONTACT SYMANTEC CUSTOMER SERVICE FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the property of Symantec, or its licensors, and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, You may make the number of copies of the Software licensed to You by Symantec as provided in Your License Module. Your License Module shall constitute proof of Your right to make such copies;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and

E. use the Software in accordance with any additional permitted uses set forth, below.

You may not:

A. copy the printed documentation that accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

E. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

G. use the Software in any manner not authorized by this license; nor

H. use the Software in any manner that contradicts any additional restrictions set forth, below.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

There are technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures to protect Symantec against software piracy. This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a machine to not more than a finite number of times for a finite number of machines. This License and the Software containing enforcement technology require activation as further set forth during installation and in the Documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation, You will provide Your unique product key accompanying the Software and PC configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the Documentation, or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event You are not able to activate the Software, You may contact Symantec Customer Support at the URL, or and telephone number provided by Symantec during activation, or as may be set forth in the Documentation.

4. Sixty (60) Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes) at any time during the sixty (60) day period following the date of purchase.

5. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

6. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

7. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items,” as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

8. Export Regulation:

The Software and its related documentation, including technical data, may not be exported or re-exported in violation of the U.S. Export Administration Act, its implementing laws and regulations, the laws and regulations of other U.S. agencies, or the export and import laws of the jurisdiction in which the Software was obtained. Export to any individual, entity, or country specifically designated by applicable law is strictly prohibited.

9. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

ADDENDUM FOR NORTON GHOST

This addendum adds certain sections to the Symantec Software License Agreement specific to the Software's Norton Ghost component ("Norton Ghost"). These additional sections apply only to Norton Ghost.

In addition to Sections 1(A)-(D) under the heading "You may" in the Symantec Software License Agreement, you may:

(i) use Norton Ghost on one computer to clone, or apply an image of, a hard drive on that computer, or a portion thereof, to another hard drive on the same computer. If a License Module accompanies, precedes, or follows this license, you may make and use that number of copies of Norton Ghost licensed to you by Symantec as provided in your License Module on an equal number of individual computers pursuant to the terms of this license. Your License Module shall constitute proof of your right to make and use such copies;

(ii) use Norton Ghost on that same computer to create an image file of a hard drive on that computer and store the image file on removable media for disaster recovery purposes;

(iii) use Norton Ghost to create a boot disk as described in the documentation for reapplying the hard drive image that was created for disaster recovery purposes to the hard drive on that same computer; or

(iv) use Norton Ghost to clone a hard drive from that same computer to a replacement computer, in the manner described in the software documentation, and to use Norton Ghost on the replacement computer provided that Norton Ghost has been removed from the original computer.

In addition to Sections 1(A)-(F) under the heading "You may not" in the Symantec Software License Agreement, you may not use Norton Ghost commercially or non-commercially for the purpose of creating multiple computers or hard drives not connected to the original computer, with similar or identical configurations to that of the original computer or hard drive.

All of the other sections of the Symantec Software License Agreement above shall apply to Norton Ghost.

Contents

Responding to emergencies

1

If you have an emergency, read these sections to try to find the solution to your problem.

Common problems include:

- Virus *threats*
- Trouble restarting your computer
- Lost or missing files
- Possible disk damage

If you purchased this product to address any of the problems listed above, read these sections first. Immediate installation of the product may not always provide the best solution to your problem.

If your product won't install

⚠ You must be running Windows in order to install your Symantec product.

If you try to install and your computer has a virus and you choose not to run the Symantec Pre-Install Scanner, start over and run the Symantec Pre-Install Scanner as directed.

If you can't run the Symantec Pre-Install Scanner, but you can connect to the Internet, go to http://security.symantec.com and run virus detection from the Symantec Security Check Web site.

See "If your computer won't start" on page 15.

If you can't start your computer, you need to start from an uninfected disk and scan for viruses.

Once the virus has been repaired, delete the installation files that were left behind in the temporary folder after you tried to install the first time.

To delete remaining installation files

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run dialog box, type **%TEMP%**
3. Click **OK**.
4. In the Temp window, select all of the files that can be deleted. If system files are open, you will not be able to delete them. Just delete the ones that you can.
5. Click **Delete**.
6. Close the window.
7. After you delete the temporary files, begin installation again and run the Symantec Pre-Install Scanner to be sure that you have removed all of the viruses.

If your computer won't start

If you have a virus or threat on your computer, you need to start the computer from an uninfected disk to remove the virus.

Suggestion	For more information
Restart from the CD and scan your computer's hard disk for viruses.	See "Scan for viruses using the CD" on page 15.
Start your computer by using your Rescue Disks if you created them. ❗ Rescue Disks are available only for Windows 98/Me.	See "Create and use Rescue Disks" on page 86.

Scan for viruses using the CD

❗ You might need to change your computer's BIOS Setup options to start from the CD-ROM drive. To do so, see the documentation that came with your computer.

To start from the CD and scan for viruses

1. Insert the CD into the CD-ROM drive.
2. Restart your computer.
   Your computer displays the following information:
   - 1 Boot from Hard Drive
   - 2 Boot from CD-ROM
3. Press **2 Boot from CD-ROM** to restart from the CD.
   After the computer restarts, the Emergency program automatically begins to scan for and remove viruses.
4. When Norton AntiVirus has finished scanning, remove the CD from your CD-ROM drive.

If your disk is damaged

If you are unable to start your computer because of a virus threat or damage to your hard disk, you can use Norton SystemWorks tools to start your computer and repair your hard disk.

If Windows doesn’t start

If you are having startup or disk problems, you can do one of the following:

Suggestion	For more information
Restart your computer from your Windows Startup Disk, and then use the utilities on the CD to repair your problem.	See “If you have your Windows Startup Disk” on page 17.
If you have access to another computer, you can use the CD to create a set of Emergency Disks.	See “Create Emergency Disks” on page 25.
If you suspect that your computer has a virus, you can restart from the CD and scan your computer’s hard disk for viruses. ⚠ The DOS-based Norton AntiVirus, if run from the CD, uses the virus definitions from the CD, and will not be as up-to-date as virus definitions that are downloaded using LiveUpdate.	See “Scan for viruses using the CD” on page 15.
Restart your computer from a set of Emergency Disks and repair your hard disk using DOS-based Norton Utilities tools. ⚠ DOS programs do not support NTFS formatted disks.	See “If you have access to another computer” on page 17.

If you have your Windows Startup Disk

See "Troubleshoot disk errors in Windows 98/Me" on page 306.

If you have the Windows Startup Disk that came with your computer, you can restart from it and run the *DOS-based* Norton Disk Doctor, UnErase, UnFormat, and Disk Editor from the CD.

To learn how to create a Windows Startup Disk, consult the instruction manual that came with your computer.

To start from your Windows Startup Disk and run DOS-based utilities from the CD

1 Insert the Windows Startup Disk into your floppy disk drive.

2 Insert the Symantec CD into the CD-ROM drive.

See "Troubleshoot disk errors in Windows 98/Me" on page 306.

3 Restart your computer.
When your computer restarts, the drive letters might have changed from their normal designations.

See "DOS-based troubleshooting list" on page 306.

4 At the DOS command prompt, start the Norton Utilities tool that you want to use.

If you have access to another computer

See "Create Emergency Disks" on page 25.

If you have access to another computer, you can use the CD to create a set of Emergency Disks. These disks can be used to restart your computer and repair damage to your hard disk.

To restart from Emergency Disks and run DOS-based utilities

1 Insert Emergency Disk 1 into your floppy disk drive.

See "Troubleshoot disk errors in Windows 98/Me" on page 306.

2 Restart your computer.
When your computer restarts, the drive letters might have changed from their normal designations.

3 At the DOS command prompt, start the Norton Utilities tool that you want to use.

If a file is deleted or missing

If you can't find a file, you can search for it with UnErase before installing Norton SystemWorks. In Windows 98/ Me, you can run UnErase Wizard from the CD. In other Windows versions, you can use the DOS-based version of UnErase to recover erased files on DOS formatted disks.

To avoid overwriting missing files, do not install Norton SystemWorks if you haven't already. If you are able to run Windows, you can run UnErase Wizard from the CD.

Problem	**Suggestion**
A file that you wanted to keep has disappeared or been deleted and you don't have a backup copy.	Use UnErase Wizard to search for and recover it. To avoid this problem in the future, keep up-to-date backups of your files. See "Recovering missing or erased files" on page 219.
You can't start Windows and need to recover files from a DOS disk.	Create an Emergency Disk set and use the DOS version of UnErase. See "Create Emergency Disks" on page 25. See "Troubleshoot disk errors in Windows 98/Me" on page 306.
You need to remove unwanted files.	Use Norton CleanSweep to improve your computer's performance by removing files and programs that you no longer need, while protecting the files that you do need. See "Removing unwanted files and programs" on page 257.

Problem	Suggestion
You need to recover data from unrecoverable files.	Use Disk Editor (Diskedit.exe), which is capable of accessing virtually any area of a hard or floppy disk. You can edit files and directories, the partition table, the boot record, and the file allocation tables (FATs) on most hard disks. You can treat any group of clusters or sectors as an object to view and edit. ⚠ Disk Editor requires that you are familiar with the inner workings of disks. You must understand what you are doing before you edit any area of a disk. Otherwise, you could make the data on the disk inaccessible. The *Norton SystemWorks User's Guide* PDF on the CD contains instructions for using Disk Editor. See "Access the User's Guide PDF" on page 94.

If you need to revert a damaged disk

Use Norton GoBack to return your system to a time and date before trouble began. Or, if you have created a Ghost image, you can use Norton Ghost to return your system to a state that can also recover damaged disks.

When to use Norton GoBack

See "About reverting a disk" on page 146.

If your computer experienced a problem due to a bad installation or system crash, use Norton GoBack to revert your hard disk to a specific date and time before the problem occurred.

⚠ To be able to restore your computer to a past date and time, Norton GoBack must already be installed and enabled on your hard disk.

When to use Norton Ghost

See “Copying and cloning disk images” on page 279.

Use Norton Ghost to create disk image clones that can be used to recover lost files or damaged disks.

To recover using Norton Ghost, it must be installed and you must have already created a Ghost image of your disk.

When to run disk utilities from the CD

See “Start utilities from the CD” on page 68.

In some situations, running utilities from the CD lets you perform more comprehensive activities on your hard disk. You can run utilities from the CD when you want to repair a damaged disk or file and not increase the damage by running programs from your hard disk.

Run Norton Disk Doctor from the CD

Examine your computer’s hard disks by running Norton Disk Doctor from the CD utilities.

To run Norton Disk Doctor from the CD

1 Insert the CD into your CD-ROM drive.

If your computer is not set to automatically open a CD, you will have to open it yourself.

2 In the CD window, click **Launch Utilities From CD**.

Do not click Install Norton SystemWorks. If you are trying to repair a damaged disk, installing Norton SystemWorks might overwrite information on your hard disk.

3 In the CD Utilities window, click **Norton Disk Doctor**.

4 In the Norton Disk Doctor window, select the drives that you want to diagnose.

See “Types of Norton Disk Doctor tests” on page 210.

5 Change any other settings for the examination.
If you are examining a disk for a specific problem, you can reduce the number of tests that Norton Disk Doctor normally performs.

6. Click **Diagnose**.
   Norton Disk Doctor examines the selected disk.
7. Follow the on-screen instructions as Norton Disk Doctor identifies and fixes any problems found on your disk.
8. When the examination and repairs are complete, click **Close**.
9. In the CD Utilities window, click **Exit**.
10. Close the CD window.
11. Remove the CD from your CD-ROM drive.
12. Restart your computer.

After recovering from an emergency

When your computer is stable, you can install Norton SystemWorks and perform the following activities.

Action	Why you should do it
Install Norton SystemWorks	Once you've repaired the damage to your computer, you can install Norton SystemWorks and fix any remaining problems. See "Installing Norton SystemWorks Professional" on page 43.
Update virus protection	After you install Norton SystemWorks, run LiveUpdate to ensure that you have the most updated virus definitions and program files. See "Keeping current with LiveUpdate" on page 169.
Perform a One Button Checkup	One Button Checkup tests for common problems on your computer. See "Perform a One Button Checkup" on page 78.
Repair disk problems	Use Norton Disk Doctor to repair disk damage. See "Check your disk with Norton Disk Doctor" on page 206.
Recover missing files	Use UnErase Wizard to recover missing files. See "Recover a file with UnErase Wizard" on page 221.
Optimize your hard disks	Fragmented files can slow your computer and cause problems. Speed Disk defragments and optimizes your hard disks. See "Optimize your hard disks" on page 230.
Set a virus protection schedule	Schedule Norton AntiVirus to scan your computer regularly to ensure that it is protected. See "Schedule scans" on page 184.

Action	Why you should do it
Set Norton System Doctor sensors	Norton System Doctor sensors let you monitor different aspects of your computer's activity so that you can make adjustments to the number of programs that are running and to the available space and fragmentation level of your hard disk. See "Monitor your computer's health" on page 203.
Maintain a disk history with Norton GoBack	Norton GoBack is included on the CD but must be installed separately. It tracks every change that you make on your computer and lets you revert your hard disk to an earlier state if a problem occurs after you install software or experience a virus attack. See "Revert your hard disk" on page 147.
Create an image of your hard disk with Norton Ghost	Once you've repaired the damage to your hard disk with Norton Disk Doctor and Norton AntiVirus, you might want to clone an image of your hard disk with Norton Ghost. You can copy disk images to removable media, and then restore entire images or individual files and directories. Norton Ghost lets you restore your hard disk to the cloned state if something goes wrong. You can also use the standalone Ghost Explorer utility to restore individual files or entire directories from a cloned disk image. If you are not able to repair damage to your hard disk, a cloned image could let you salvage data. You could then use Ghost Explorer and UnErase to restore files to a new hard disk. See "Copying and cloning disk images" on page 279.

Stay prepared for emergencies

It is important that you are prepared in case your computer is infected by a virus or damaged due to a system crash.

To prepare for emergencies

❖ Do the following:

Regularly back up files and keep more than just the most recent backup.	See your Windows operating system tools or another disk backup program for information on backing up your hard disk.
If your computer cannot start from a CD, create a set of Emergency Disks from which you can start your computer and scan for viruses.	See "Create Emergency Disks" on page 25.
If you are using Windows 98/Me, you can also create a set of Rescue Disks with which you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems and Norton Utilities tools to recover from system crashes or recover lost files.	See "Create and use Rescue Disks" on page 86.
Install Norton GoBack so that you can revert your hard disk to a safe point in case your computer crashes.	See "Install Norton GoBack" on page 57.

Create Emergency Disks

Emergency Disks are used to start your computer in case of a problem. If your computer can start from a CD, you can use the product CD in place of Emergency Disks and do not need to create them.

If you downloaded the software or do not have a CD, the program for creating Emergency Disks (NED.exe) is included in the download. Navigate to the location to which you downloaded the software and begin with step 3 of these instructions.

See "If you need to use Emergency Disks" on page 26.

If you cannot start your computer from a CD, you can use these instructions to create Emergency Disks on another computer or go to http://www.symantec.com/techsupp/ebd.html and download the Emergency Disk program. Follow the instructions included in the download to create the Emergency Disks.

⚠ You will need several formatted 1.44-MB disks.

To create Emergency Disks from the CD

1. Insert the CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Support** folder.
4. Double-click the **Edisk** folder.
5. Double-click **NED.exe**.
6. In the welcome window, click **OK**.
7. Label the first disk as instructed and insert it into drive A.
8. Click **Yes**.
9. Repeat steps 7 and 8 for the subsequent disks.
10. When the procedure is complete, click **OK**.
11. Remove the final disk from drive A.
12. Test the first disk in the set to ensure that you can restart your computer with it.
13. Store the Emergency Disk set in a safe place.

If you need to use Emergency Disks

See "Create Emergency Disks" on page 25.

If you have not created Rescue Disks, you can use Emergency Disks to restart your computer and scan for viruses or run DOS-based recovery utilities.

To use Emergency Disks

1. Insert Emergency Disk 1 into drive A and restart your computer.
   The Emergency program runs in DOS.
2. Select the program that you want to run.
   For DOS program help, press the **F1** key while you are running the program.
3. Follow the on-screen instructions for inserting and removing the Emergency Disks.
4. When the Emergency program is done, remove the Emergency Disk from drive A and restart your computer.

1

Getting started

Feature summary

2

Use the information in this section to familiarize yourself with the product.

This section includes:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

Activation protects you

Product activation is a technology that protects users from pirated or counterfeit software by limiting use of a product to those users who have acquired the product legitimately. Product activation requires a unique product key for each installation of a product. You must activate the product within 15 days of installing it.

Product activation is completely separate from registration. Your activation information and registration information reside on separate servers, with no link between the different sets of data.

When to activate your product

During installation, you are asked to enter a product key. After you have installed the product, activate it by sending the product key to the Symantec servers.

You can activate your product by clicking Activate Now in the Configuration Wizard that runs immediately after installation. If you choose not to activate at that time, you will receive *alerts* that will remind you to activate the product. You can click Activate Now in the alerts to activate the product. Activation should take just a few minutes.

⚠ If you do not activate the product within 15 days of installing it, the product will stop working. You can activate it after the 15 days have elapsed.

Locate the product key

The product key can most frequently be found on a sticker on your CD sleeve. If it is not there, then it will be on an insert in your product package. If you have purchased the product on DVD, look for the sticker on your DVD package. If you have *downloaded* the product from the Symantec Store, the product key is stored on your computer as part of the download process.

Problem-solving features

Norton SystemWorks is a suite of Symantec products that expertly maintain and protect your computer while boosting its performance. New features let you:

Perform diagnostic tests using One Button Checkup	Providing a comprehensive analysis of your computer, One Button Checkup finds and solves disk, file, and Windows system problems, performance issues, and virus vulnerabilities. You can schedule automatic checkups, view a history of previous repairs, and undo them if necessary. See "Perform a One Button Checkup" on page 78.
Scan your computer for unnecessary files with Web Cleanup	Web Cleanup cleans out your computer after you browse the Internet with Internet Explorer. You can delete history files and cookies, or view them and decide which ones to keep. See "About Web Cleanup" on page 135.
Create a full system backup using Norton Ghost	For technically advanced users, Norton Ghost quickly restores a computer to the last backup copy. You can install Norton Ghost from the CD. See "Copying and cloning disk images" on page 279.
Run tests to measure your computer's performance	This trial version of PerformanceTest runs benchmark and diagnostic tests that compare your computer's performance with the performance of other typical computer systems. See "Install other products from the CD" on page 56.

View processes that are currently running on your computer	Process Viewer displays the activities that are currently running in your computer's memory. Among other things, it gives you the full list of DLLs for each running process, including the full path and version information for each loaded module. It also shows memory, threads, and DLL usage for every process. Process Viewer is installed with Norton SystemWorks. See "Access Extra Features" on page 69.
Use Symantec Web-based tools	Web-based tools provide additional ways to assist you and protect your computer. They include the following: ■ Symantec Security Check Tests your computer's exposure to online security intrusions and virus threats ■ Tech24.com Provides online advice and assistance for your computer problems and questions See "Access Extra Features" on page 69.

Norton Utilities features

Norton Utilities includes the following features:

Speed Disk (Windows 98/Me/2000/XP)	Improves system performance by reorganizing the contents of your disk so that your files are stored in adjacent clusters, improving chances of recovering erased files. It works with Windows 98 Application Launch Accelerator to make your programs load faster. See "Optimize your hard disks" on page 230.
Norton Optimization Wizard (Windows 98/Me)	Optimizes the internal structure of the registry, reducing its size on your hard disk and speeding access time to the vital information it contains. It also sets your swap file's minimum size to the optimum setting for your system and works with Speed Disk to move the swap file to the front of your hard disk for maximum efficiency. See "Optimize registry and swap files" on page 241.

Norton System Doctor (Windows 98/Me/ 2000/XP)	Monitors and analyzes various parts of your computer, including disk and CPU usage, disk integrity, system integrity, network throughput, Internet site access time, and more. See "Monitor your computer's health" on page 203.
Norton Disk Doctor (Windows 98/Me/ 2000/XP)	Performs a series of surface analysis tests to ensure the integrity of your disks and repairs problems. It works alone or with Norton System Doctor, continuously monitoring for disk problems and alerting you when they occur. See "When to use Norton Disk Doctor" on page 204.
Norton WinDoctor (Windows 98/Me/ 2000/XP)	Performs a series of tests to diagnose and fix most Windows problems. It works alone or with Norton System Doctor, continuously checking for Windows problems, and alerts you when they occur. See "Find and fix Windows problems" on page 210.
System Information (Windows 98/Me/ 2000/XP)	Reports on common device information as well as hard-to-find details about your computer, including memory, logical and physical characteristics of your disks (including partitions), network connections, and your Internet connection. See "Use System Information" on page 253.
Image (Windows 98/Me)	Creates a snapshot of critical disk information: The boot record, file allocation tables (FAT), and root directory data. UnErase Wizard, UnFormat, and Norton System Doctor use this information. For more information, see the online Help.
Norton File Compare (Windows 98/Me)	Compares two versions of the same file and displays the differences. For more information, see the online Help.

Registry management (Windows 98/Me)	Norton Registry Tracker monitors changes to your computer's critical setup data and startup files, including Windows registry keys and .ini files. Norton Registry Editor lets you edit the Windows registry. Its Undo feature makes it safer to use than other registry editing tools. For more information, see the online Help.
DOS-based repair and recovery (Windows 98/Me MS-DOS or PC-DOS)	Fix computer problems using DOS-based Norton Disk Doctor, UnErase, UnFormat, and Disk Editor. These programs are also provided on Rescue Disks and Emergency Disks that you can create from tools on the CD. See "Troubleshoot disk errors in Windows 98/Me" on page 306.

Norton CleanSweep features

Norton CleanSweep consists of the following tools that you can use individually or in combination:

Fast & Safe Cleanup	Frees hard disk space by finding and deleting files that are safe to remove, such as temporary files, Internet browser cache files, and the files in the Windows Recycle Bin. See "Use Fast & Safe Cleanup" on page 258.

Smart Sweep/ Internet Sweep	Smart Sweep monitors your computer for program installations, and keeps track of all the locations where programs install files and settings. Backup Wizard and Restore Wizard use this information to ensure that all files belonging to a program are included in a backup or restore operation. See "Removing unwanted files and programs" on page 257. Internet Sweep keeps track of cache files, cookies, plug-ins, and ActiveX controls installed from the Internet. See "Uninstall programs that were downloaded from the Internet" on page 266.
Backup Wizard/ Restore Wizard	Backup Wizard compresses and backs up infrequently used programs. Restore Wizard ensures that all of a program's related files are restored when you want to use the program again. See "Backing up and restoring programs" on page 273.

Advanced Utilities features

Norton Utilities keeps your computer working its best by finding, solving, and preventing Windows and disk problems. The UnErase and Wipe Info tools include the following features:

UnErase Wizard (Windows 98/Me/ 2000/XP)	Locates and recovers files that are protected by Norton Protection or the Windows Recycle Bin. See "About UnErase Wizard" on page 220.
Norton Protection (Windows 98/Me/ 2000/XP)	Adds extra data recovery protection to the Recycle Bin. When used in conjunction with UnErase Wizard, it provides the most complete recovery system for all deleted or overwritten files. See "About Norton Protection" on page 219.
Wipe Info (Windows 98/Me/ 2000/XP)	Permanently removes unwanted files so that they never can be recovered by a file recovery program. It can also wipe the free space on your hard disk to ensure that previously deleted information is not left on your hard disk. See "Eliminating data permanently" on page 247.

Web Tools features

With Web Tools you can delete unneeded files that have accumulated during Internet sessions, including cookies, cache files, and Internet history files. You can also prevent interruption during dial-up Internet sessions. Web Tools include the following features:

Web Cleanup	Scans your computer for unnecessary files that have been left on your computer after you browse the Internet with Internet Explorer. You can delete these files or view them and decide which ones to keep. See “About Web Cleanup” on page 135.
Connection Keep Alive	Helps maintain your dial-up connection to the Internet, even when your computer is idle. See “About Connection Keep Alive” on page 141.

Virus and threat protection features

Norton AntiVirus provides comprehensive virus prevention, threat detection, and repair software for your computer. It automatically detects and repairs known viruses. Norton AntiVirus detects viruses and other potential risks in instant messenger attachments as well as in email messages, Internet downloads, and other files. Easy updating of the *virus definitions* over the Internet keeps Norton AntiVirus prepared for the latest *threats*.

Norton AntiVirus now includes expanded threat detection of both known and emerging threats, such as spyware and other files that could put your computer at risk. Norton AntiVirus also scans files inside of compressed files.

As always, Norton AntiVirus features continually monitor your computer and protect it from known and unknown threats.

Feature	Description
Auto-Protect	■ Loads into memory when Windows starts, providing constant protection while you work. ■ Checks for viruses every time that you use software programs on your computer, insert floppy disks or other removable media, access the Internet, or use document files that you receive or create. ■ Monitors your computer for any unusual symptoms that may indicate an active threat. See "What to do if a virus is found" on page 189.
Virus protection updates	Updates your virus definitions automatically. See "About protection updates" on page 170.
Compressed file protection	Detects and repairs viruses inside of compressed files. See "What to do if a virus is found" on page 189.

Feature	Description
Email protection	Protects incoming and outgoing email messages, preventing your computer and other computers from infection. See "What to do if a virus is found" on page 189.
Instant messenger protection	Scans for and detects viruses in instant messenger attachments. See "What to do if a virus is found" on page 189.
Bloodhound technology	Detects new and unknown viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data that is contained in the file. See "What to do if a virus is found" on page 189.
Password protection	Protects Norton AntiVirus options from unauthorized changes. See "Password protect Norton AntiVirus options" on page 124.

Norton Password Manager features

Norton Password Manager fills forms automatically and protects your passwords and other confidential information in encrypted files on your computer.

Norton Password Manager includes the following features:

A single profile password	You no longer need to remember passwords for all of the Web sites and programs that require them. After you have added your passwords and other information to a Norton Password Manager profile, you use a single profile password.
Password strength assistance	To ensure that your profile password is secure, a message appears if the password that you create is not strong.
Address and credit card wizard	The program steps you through the process of adding addresses, telephone numbers, and credit card information.
Privacy for shared computers	Norton Password Manager supports multiple profiles, all of which can have different passwords.
Secure portability	You can create backups of your profile data and restore the backups to another activated installation of Norton Password Manager.
Convenient access	When you are signed in to a profile, the Norton Password Manager icon appears in the Windows system tray for easy access when you need to sign in to a program or Web page.
Automatic updates	If program updates are issued, LiveUpdate retrieves and installs them automatically.

Norton Ghost features

Norton Ghost is a fast and reliable software solution to satisfy all of your computer disk cloning and copying needs. The high-performance utilities in Norton Ghost help you upgrade, back up, and recover entire disks or selected partitions. Norton Ghost can determine the partition sizes for the destination drive automatically.

Creating a Norton Ghost image helps to protect your data from computer disasters. The intuitive Windows interface lets you create backup images of your hard disk or selected partitions. You can clone directly between two computers using a network, USB, or parallel connection. Norton Ghost is based on the robust cloning technology of Symantec Ghost Enterprise.

See “Copying and cloning disk images” on page 279.

Norton GoBack features

Norton GoBack includes the following feature:

Revert your hard disk to a previous date or time	Norton GoBack Personal Edition records all changes to your hard disk and, if your computer experiences a problem, lets you revert your disk to an earlier safe point before the problem occurred. Norton GoBack has a separate installer on the CD. See "Reverting your hard disk" on page 145.

Installing Norton SystemWorks Professional

3

Before installing Norton SystemWorks, take a moment to review the system requirements. Windows 98/Me users should have several blank 1.44 MB disks available to make Rescue Disks.

If you think you have lost or destroyed data, or you purchased Norton SystemWorks because there is a problem with your hard disk, do not install the program and do not start Windows. You may overwrite and destroy data that you want to recover. See "Responding to emergencies" on page 13.

System requirements

Installation of Norton SystemWorks is not supported on Windows 95/NT 4.0, Macintosh, Linux, BSD, UNIX, or server versions of Windows 2000/XP computers. Norton Ghost supports Windows NT, OS/2, and Linux in addition to the operating systems that are supported by Norton SystemWorks.

If you are planning to upgrade your Windows operating system from Windows 98/Me to Windows 2000/XP, you must uninstall Norton SystemWorks first and then reinstall after the upgrade is complete.

To use Norton SystemWorks Professional, your computer must have one of the following Windows operating systems:

- Windows 98, 98SE
- Windows Me

- Windows 2000 Professional
- Windows XP Professional or Windows XP Home Edition

Your computer must also meet the following minimum requirements.

Operating system	Requirements
Windows 98/98SE/ Me	- 133-MHz processor for Windows 98; 150-MHz processor for Windows Me - 32 MB of RAM - 180 MB of available hard disk space - CD-ROM or DVD-ROM drive - Internet Explorer 5.01 with Service Pack 2 or later (6.0 recommended)
Windows 2000 Professional Edition	- 133-MHz or higher processor - 64 MB of RAM - 180 MB of available hard disk space - CD-ROM or DVD-ROM drive - Internet Explorer 5.01 with Service Pack 2 or later (6.0 recommended)
Windows XP Professional/Home Edition Service Pack 1	- 300-MHz or higher processor - 128 MB of RAM - 180 MB of available hard disk space - CD-ROM or DVD-ROM drive - Internet Explorer 5.01 with Service Pack 2 or later (6.0 recommended)

If you are installing on Windows 2000/XP, you must install with administrator privileges.

Supported email clients

Email scanning is supported for any standard *POP3*-compatible and SMTP-compatible email client including:

- Microsoft Outlook Express version 4, 5, or 6

- Microsoft Outlook 97/98/2000/XP
- Netscape Messenger version 4, Netscape Mail version 6
- Eudora Light version 3, Eudora Pro version 4, Eudora version 5
- Pegasus 4

Unsupported email programs

Norton AntiVirus does not support the following email clients:

- IMAP
- AOL
- POP3 with Secure Sockets Layer (SSL)
  See the online Help for more information about Secure Sockets Layer connections.
- Web-based email such as Hotmail and Yahoo!
- Lotus Notes

Send email through an SSL connection

Norton AntiVirus does not support email connections using Secure Sockets Layer (SSL). SSL is a Netscape protocol designed to provide secure communications on the Internet. If you use an SSL connection, you are not protected by Norton AntiVirus.

To send email messages through SSL connections, disable incoming and outgoing email protection in Norton AntiVirus.

To send email through an SSL connection

1 At the top of the main window, click **Options**.
  If a menu appears, click **Norton AntiVirus**.

  If you set a password for Options, Norton SystemWorks Professional asks you for the password before you can continue.

2 In the Options window, click **Email**.

3 Click **OK**.

4 Uncheck **Scan incoming Email (recommended)**.

5. Uncheck **Scan outgoing Email (recommended)**.
6. Resend your email.

Supported instant messenger clients

The following instant messenger clients are supported:

- AOL Instant Messenger, version 4.7 or later
- Yahoo! Messenger, version 5.0 or later
- MSN Messenger, versions 4.6 and 4.7
- Windows Messenger, version 4.6 or later for Windows XP

Norton Ghost requirements

For disaster recovery using Norton Ghost, you must have one of the following drive types:

- Floppy disk drive
- Writable CD-ROM or DVD-ROM drive

To use the Norton Ghost backup capability, you must have one of the following devices and appropriate media:

- An available local *partition*
- A secondary or external hard disk, Zip disk, or other mass storage device
- CD-R/RW or DVD-R/RW device (DVD supported formats include +R, +RW, -R, and -RW)
- Access to a mapped network drive
- SCSI or ATAPI (QIC157) tape device

Norton GoBack requirements

Norton GoBack Personal Edition requires the following:

- 200 MB of available hard disk space
- Approximately ten percent of your total hard disk space for Norton GoBack history (configurable)

PerformanceTest requirements

PerformanceTest by Passmark requires DirectX 8.0.

Prepare your computer

See “Create Emergency Disks” on page 25.

Before you install Norton SystemWorks, prepare your computer. If your computer cannot start from a CD, create Emergency Disks.

See “If you need to uninstall Norton SystemWorks” on page 60.

If you have an earlier version of Norton SystemWorks, Norton AntiVirus, or Norton Ghost installed, the new version automatically removes the earlier version. If your version is earlier than 2002, you must uninstall it before installing the new version. If you have Norton AntiVirus 2002 installed, you can transfer your existing option settings to the new version of the program in Norton SystemWorks.

Before you install Norton SystemWorks, use these suggestions to prepare your computer:

- If you have any other antivirus programs on your computer and you plan to include Norton AntiVirus as part of your installation of Norton SystemWorks, you must uninstall the other antivirus programs and restart your computer before installing Norton SystemWorks.
  To uninstall other antivirus programs, see the user documentation that came with each program.
- Close all other Windows programs before installing Norton SystemWorks, including those programs displayed in the Windows system tray.

Before installation, you should do the following:

Task	For more information
Scan for viruses or examine your hard disk while you have restarted from the CD.	Allow the Symantec Pre-Install scanner to run during installation. See "Install Norton SystemWorks" on page 48.
Run Norton Disk Doctor, Norton WinDoctor, or other utilities from the CD.	See "Start utilities from the CD" on page 68.
If your computer cannot start, use another computer to create Emergency Disks.	See "Create Emergency Disks" on page 25.

Install Norton SystemWorks

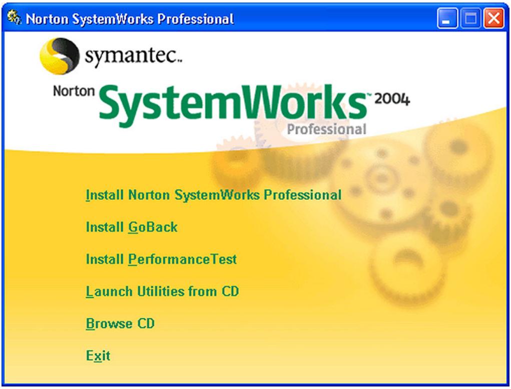
Install Norton SystemWorks from the CD or if you downloaded your copy of the product, follow the instructions on the Web page.

If you have not already done so, close all other Windows programs.

To install Norton SystemWorks from the CD

1 Insert the CD into the CD-ROM drive.

If your computer is not set to automatically open a CD, you will have to open it yourself.



2 In the Norton SystemWorks window, click **Install Norton SystemWorks Professional**.

3 In the Scan for Viruses dialog box, click **Yes** to scan your computer with Norton AntiVirus before installing Norton SystemWorks.
This scan could take several minutes.

4 In the Symantec Pre-Install Scanner window, review the progress of the scan and note any messages.
If Norton AntiVirus detects a virus, it prompts you to delete each file individually.

5 Click **Delete** for each file that you want to delete.

6 After the scan completes, view the results in the scanresults - Notepad window, then exit Notepad.

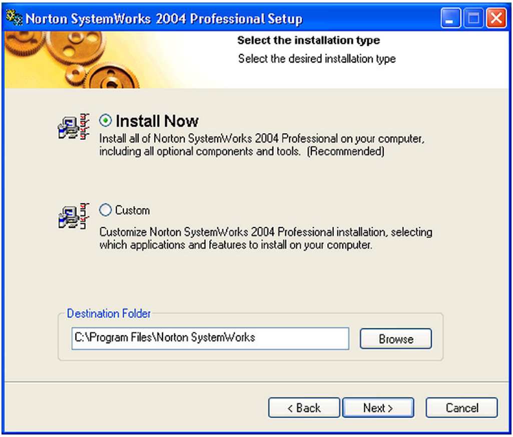
7 In the Norton SystemWorks 2004 Setup window, read the welcome message, then click **Next** to continue with the installation.

8 Read the License Agreement, then click **I accept the license agreement**.
If you decline, you cannot continue with the installation.

9 Click **Next**.

See "Activation protects you" on page 30.

10 In the Activation window, type the product key for activation, then click **Next**.



Norton SystemWorks 2004 Professional Setup

Select the installation type

Select the desired installation type

● Install Now

Install all of Norton SystemWorks 2004 Professional on your computer, including all optional components and tools. (Recommended)

○ Custom

Customize Norton SystemWorks 2004 Professional installation, selecting which applications and features to install on your computer.

Destination Folder: C:\Program Files\Norton SystemWorks

11 Select an installation type. Your options are:

Install Now	This is the recommended option. It installs all the tools in Norton SystemWorks. (!) Norton GoBack and PerformanceTest must be installed separately. See "Install other products from the CD" on page 56.
Custom	This option lets you omit tools from the installation. See "Customize installation" on page 51.

12 To continue with the default installation settings, ensure that Install Now is selected, then click **Next**.

13 To select a different Destination Folder, click **Browse**, select a directory, then click **Next**.
If you are upgrading from Norton AntiVirus 2002 or 2003, you can keep your option settings.

14 Click **Yes** to keep your option settings, then click **Next**.
If you have Norton AntiVirus 2001 or 2002 Professional Edition installed on your computer, you can keep the Symantec AntiVirus for Palm OS component installed.

15 Click **Yes** to keep the component installed, then click **Next**.

16 Review the summary of your installation selections, then click **Next**.
The Norton SystemWorks Setup window displays installation progress. Depending on your computer system speed, this will take several minutes.

17 Scroll through the Readme text, then click **Next**.
At the end of installation, you are instructed to remove any disks from their drives (including the program CD).

18 Click **Finish** to complete the installation.

After installation, you might have to restart your computer to enable Norton SystemWorks automatic programs, including Norton Password Manager and Norton AntiVirus Auto-Protect.

Customize installation

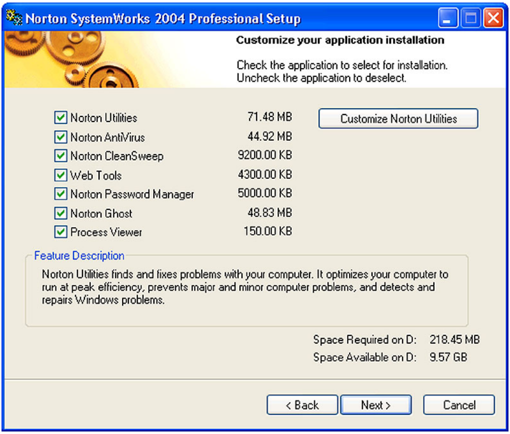
If you want to customize installation, you can select or deselect the programs that you want to install.

To customize installation

See "Install Norton SystemWorks" on page 48.

1 Complete steps 1 through 10 under To install Norton SystemWorks from the CD.

2 In the Installation Type window, click **Custom**.


Norton SystemWorks 2004 Professional Setup

Customize your application installation

Check the application to select for installation.
Uncheck the application to deselect.

☑ Norton Utilities	71.48 MB
☑ Norton AntiVirus	44.92 MB
☑ Norton CleanSweep	9200.00 KB
☑ Web Tools	4300.00 KB
☑ Norton Password Manager	5000.00 KB
☑ Norton Ghost	48.83 MB
☑ Process Viewer	150.00 KB

Customize Norton Utilities

Feature Description

Norton Utilities finds and fixes problems with your computer. It optimizes your computer to run at peak efficiency, prevents major and minor computer problems, and detects and repairs Windows problems.

Space Required on D: 218.45 MB
Space Available on D: 9.57 GB

See "Problem-solving features" on page 31.

In the Customize your application installation dialog box, all programs are checked.

3 Uncheck the programs that you do not want to install, then click **Next**.

4 To customize the Norton Utilities programs that will be installed, click **Norton Utilities**, uncheck the programs that you do not want to install, then click **OK**.

5 Click **Next**.

See "Install Norton SystemWorks" on page 48.

6 Continue with steps 13 through 18 under To install Norton SystemWorks from the CD.

For Windows 98/Me, you must restart your computer after installing Norton SystemWorks.

See "Use the Information Wizard" on page 53.

If your computer needs to be restarted after Norton SystemWorks is installed, a prompt appears giving you the option to do so immediately. After restarting or if your computer does not need to be restarted, the Information Wizard appears.

After installation

You may need to restart your computer after installing Norton SystemWorks. After it restarts, the Information Wizard steps you through activation and registration, summarizes the installation settings, and completes the installation setup.

If you bought your computer with Norton SystemWorks already installed, the Information Wizard appears the first time that you start Norton SystemWorks. You must accept the license agreement that appears in the Information Wizard to activate Norton SystemWorks.

Use the Information Wizard

The Information Wizard lets you review the Norton SystemWorks settings.

If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register by using the Product Registration option on the Help menu or by using the Symantec Web site at www.symantec.com. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

1. In the welcome window, click **Next**.

   You must activate the software within 15 days.

2. On the Product Activation window, click **Activate and register your product now**.
3. Click **Next**.
4. If the Activation window appears, type your product key.
5. Make sure that your computer is connected to the Internet, then click **Next**.
6. If you purchased your computer with Norton SystemWorks already installed, you must accept the license agreement in order to use Norton SystemWorks. Click **I accept the license agreement**, then click **Next**.

7 In the first Registration window, select the Country/ Region from which you are registering.

8 If you would like information from Symantec about Norton SystemWorks, check the method by which you want to receive that information, type the corresponding email address and phone number, then click **Next**.

9 Check if you would like to receive postal mail from Symantec.

10 Type your name and address, then click **Next**.

11 Click **Finish**.

12 Review the summary of post-installation tasks and configuration settings that are set up automatically. Some of the tasks that are set up automatically include:

Run LiveUpdate	Ensures that you have the latest virus definitions. See "Keeping current with LiveUpdate" on page 169.
Create a Rescue Disk Set	If you are installing in Windows 98/ Me, you also have the option to create a Rescue Disk set. See "Create and use Rescue Disks" on page 86.
Scan for Viruses	Perform a full system scan with Norton AntiVirus. See "Manually scan disks, folders, and files" on page 180.

Schedule weekly scans of local hard drives with Norton AntiVirus and One Button Checkup	Schedule weekly scans of your local hard drives with Norton AntiVirus and One Button Checkup. You must have Microsoft Scheduler installed to use these options. If you select these options, you can change their schedules. See "Schedule scans" on page 184. See "Set Norton SystemWorks options" on page 108.
Enable scanning of compressed files by Auto-Protect	Set the option to scan compressed files automatically by Norton AntiVirus Auto-Protect. See "About Internet options" on page 121.

If you want to change any of the scheduled or startup settings, use their program options. See "Options" on page 99.

13 Click **Next**.

14 Click **Finish**.

Read the Readme file

If you didn't read the Readme file during installation, you can read it later. The Readme file contains technical tips and information about product changes that occurred after this guide was published. It is installed on your hard disk in the same location as the Norton SystemWorks product files.

To read the Readme file

1. Using Windows Explorer, navigate to the location in which your Norton SystemWorks files are installed. If you installed Norton SystemWorks in the default location, the files are in C:\Program Files\Norton SystemWorks.
2. Double-click **Readme.txt** to open the file in your text editor, which is usually Notepad or Wordpad.
3. Close the text editor when you are done reading the file.

Install other products from the CD

The CD includes a separate installer for Norton GoBack. It also includes a separate installer for PerformanceTest. After you install Norton SystemWorks and restart your computer you can install other available programs on the CD.

Before you install Norton GoBack

Before you install Nortn GoBack, back up your system and close all open programs, including antivirus applications.

When you install Norton GoBack, you can choose between Easy Install and Custom Install.

Easy Install (recommended for most users)	Allocates ten percent of each of your hard disks to Norton GoBack automatically. If you have multiple partitions (logical hard drives) on a single hard disk, Norton GoBack allocates space on the partition with the most unused space.
Custom Install	Lets you choose the hard disks that you want Norton GoBack to protect and the amount of space that you want Norton GoBack to use on each of them. If you have multiple partitions on a hard disk, Norton GoBack requires that all partitions be protected.

Install Norton GoBack

Norton GoBack typically requires ten percent of your available hard disk space. If less than twenty percent of your total hard disk space is available, Norton GoBack uses half of the available space.

ⓘ In Windows 98/Me, Norton GoBack will not install on hard disks that are running in MS-DOS Compatibility mode.

Do not use Norton GoBack with Windows 2000 Server or other servers due to the large number of server-based events that are generated.

If you are installing on Windows 2000/XP, ensure that you are logged onto the computer as an Administrator or as a user with Administrative privileges.

To install Norton GoBack

1. Insert the CD into the CD-ROM drive.
2. In the CD window, click **Install GoBack**.
3. In the GoBack Setup Wizard, click **Yes** to accept the license agreement, then click **Next**.
4. Click **Show README File** to view the Readme file, then click **Next**.
   If you do not have Adobe Acrobat Reader installed on your computer, Norton GoBack will ask you if you want to install it.
5. To install Adobe Acrobat Reader, click **Install Adobe Acrobat**, then click **Next**.
6. In the registration confirmation dialog box, ensure that your name and organization information are correct, then click **Next**.

7 Select the type of install that you want. Your options are:

Easy Install (recommended)	This option lets Norton GoBack allocate approximately ten percent of your hard disk space to its history files.
Custom Install	This option lets you specify a partition on which to install Norton GoBack, and specify the maximum amount of disk space that Norton GoBack can allocate to its history files.

8 Confirm a location for the Norton GoBack installation files, then click **Next**.

9 Confirm the hard disk on which Norton GoBack will be installed, then click **Finish**.
During this process, Norton GoBack examines your local hard disks.

10 Click **Yes** if you want a shortcut to Norton GoBack placed on your desktop.

11 Click **OK** to confirm that installation is complete.
Your computer restarts.

After you install Norton GoBack

After your computer restarts, a Norton GoBack icon appears in the Windows system tray. Norton GoBack monitors your computer without requiring any action on your part.

Norton GoBack creates a .bin file on each protected physical hard disk. If a physical hard disk has multiple partitions, Norton GoBack uses one .bin file to track all partitions on that disk. This means that if you need to revert your disk all of the partitions on the disk will be reverted.

Install PerformanceTest

You can install PerformanceTest from the CD.

To install PerformanceTest

1. In the CD window, click **Install PerformanceTest**.
2. Click **Yes** to confirm that you want to install.
3. In the Setup-PerformanceTest Wizard, click **Next**.
4. Click **Yes** to accept all of the terms of the License Agreement.
   If you decline, the installation is cancelled.
5. Do one of the following:
   - To confirm the default destination folder location, click **Next**.
   - To select a different destination folder, click **Browse**, select any directory whose name does not contain an apostrophe, then click **Next**.
6. Confirm the name of the Start Menu folder, then click **Next**.
7. In the Ready to Install window, review the installation settings, then click **Install**.
   When installation is finished, you can view the Readme file and launch PerformanceTest.
8. If you do not want to start PerformanceTest or read the Readme file immediately, uncheck these options.
9. Click **Finish**.
   PerformanceTest places an icon on your Windows desktop and on the Windows Start menu.

If you need to uninstall Norton SystemWorks

If you need to remove Norton SystemWorks from your computer, use the Add/Remove Programs option in the Windows Control Panel.

If you have no other Symantec products installed on your computer, the uninstallation process also removes the shared programs, LiveReg and LiveUpdate.

During uninstallation, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton SystemWorks

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **Norton SystemWorks**.
4. Do one of the following:
   - In Windows 98/Me, click **Add/Remove**.
   - In Windows 2000/XP, click **Remove**.
5. Click **Remove All** to confirm that you want to uninstall the product.
6. If you have files in Norton AntiVirus Quarantine, you are asked if you want to delete them. Your options are:

Yes	Deletes the quarantined files from your computer
No	Leaves the quarantined files on your computer, but makes them inaccessible

7. Click **Reboot Now**, then click **Finish**.

If you need to uninstall Norton GoBack

If you are upgrading your operating system or installing operating system Service Packs, you must first uninstall Norton GoBack. After you uninstall or disable Norton GoBack, you will not be able to use its backups to restore your hard disk.

To uninstall Norton GoBack

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **Norton GoBack**.
4. Do one of the following:
   - In Windows 2000/XP, click **Remove**.
   - In Windows 98/Me, click **Add/Remove**.
5. Click **Remove All** to confirm that you want to uninstall the product.
6. When you're finished uninstalling Norton GoBack, restart your computer.

Basics

4

Basics include general information about how to:

- Work with your Symantec product.
- Keep your computer protected.
- Customize options.
- Monitor protection activities.
- Access more information.

Check the version number

You can check the version number of your product on your computer. Use the version number to help you find more information about your product on the Symantec Web site.

To check the version number

1 Start your product.

2 Click **Help and Support**.

3 On the Help menu, click **About <your product name>**.

4 In the About dialog box, select your product name.

Activate your product

Product activation reduces software piracy and ensures that you have received genuine Symantec software.

⚠ You must activate your product within 15 days of installing it or the product will stop working.

If you did not activate your product using the Configuration Wizard, you will receive an Activation Needed *alert* every day until you activate the product.

You can activate your product from the Activation Needed alert or from the Activation option on the Help menu. Activation should take just a few minutes.

To activate your product from the Activation Needed alert

1. In the alert, click **Activate Now**.
2. Click **OK**.
3. On the Activation screen, click **Next**.
4. On the Activation Successful screen, click **Finish**.

To activate your product from the Help menu

1. At the top of the main window, click **Help and Support** > **Activation**.
2. On the Activation screen, click **Next**.
3. On the Activation Successful screen, click **Finish**.

Access Norton SystemWorks programs

Norton SystemWorks programs include One Button Checkup, Web Tools, Norton AntiVirus tools, Norton Utilities tools, Norton CleanSweep tools, Norton GoBack, and Extra Features.

All of the programs can be accessed from the main window. In addition, some programs can be accessed from the Windows Explorer toolbar, system tray, or desktop shortcut menu.

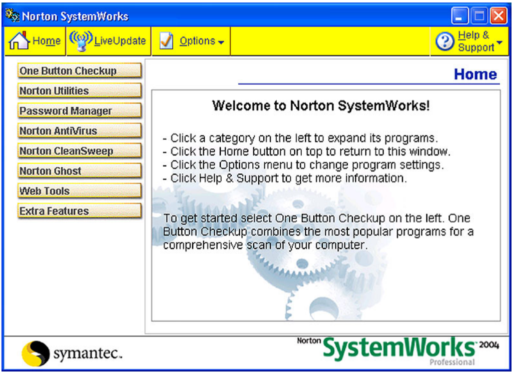
Start Norton SystemWorks

From the main window you can access the installed programs, set options, run LiveUpdate, and perform other activities.

To start Norton SystemWorks

1 Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton SystemWorks** > **Norton SystemWorks**.
   - On the Windows XP taskbar, click **Start** > **All Programs** > **Norton SystemWorks** > **Norton SystemWorks**.

- On the desktop, double-click the Norton SystemWorks icon.



Welcome to Norton SystemWorks!

- Click a category on the left to expand its programs.
- Click the Home button on top to return to this window.
- Click the Options menu to change program settings.
- Click Help & Support to get more information.

To get started select One Button Checkup on the left. One Button Checkup combines the most popular programs for a comprehensive scan of your computer.

2 On the left side of the main window, select a category, such as One Button Checkup, Norton Utilities or Web Tools.
A description or an expanded list of programs appears in the center of the window.

3 At the top of the main window, click a button. Your options are:

Home	Return to the main window's home state after running a program.
LiveUpdate	Start LiveUpdate, where you can update virus definitions, Norton SystemWorks, and any other installed Symantec products. See "Keeping current with LiveUpdate" on page 169.
Rescue (Windows 98/ Me)	Create a set of floppy disks to use in an emergency, such as when your computer won't start or if you think your computer is infected with a virus. See "Create and use Rescue Disks" on page 86.

Options	Customize general features of the Norton SytemWorks programs that you installed. You can access more options while you are running specific programs. See "Options" on page 99.
Help & Support	Access Help for Norton SystemWorks and other installed programs. See "Use online Help" on page 93.

Use Norton Tray Manager

See "About General options" on page 110.

In some versions of Windows, including Windows 98/Me, Norton Tray Manager adds an icon to the Windows system tray on the taskbar. Use Norton Tray Manager as a shortcut to open programs such as Norton AntiVirus and Norton Password Manager, and to enable or disable memory-resident programs such as Norton AntiVirus Auto-Protect, Connection Keep Alive, and Smart Sweep/Internet Sweep.

To use Norton Tray Manager

1 On the Windows desktop, move the mouse pointer over the Norton Tray Manager icon.
  Available program icons pop up from the Windows system tray area.

2 Right-click an icon, then, on the program's shortcut menu, select the option that you want.

Use the Windows desktop shortcut menu

You can access some Norton SystemWorks programs from the Windows desktop shortcut menu. The programs that appear on the shortcut menu depend on the kind of item that you select and the program features that you have installed.

To use the Windows desktop shortcut menu

1 On the Windows desktop, double-click **My Computer**.
  You can also open Windows Explorer.

2 Right-click a disk, folder, or file icon, then select an available option.
Depending on whether a disk, folder, or file is selected, the shortcut menu options are:

Scan with Norton AntiVirus	Scans your hard disk for viruses. See "Manually scan disks, folders, and files" on page 180.
System Info	Opens the System Information window when a disk, volume, or My Computer is selected. See "Viewing computer information" on page 253.
Send To > Wipe Info (Windows 98/Me)	Permanently deletes the selected item. See "Eliminating data permanently" on page 247.
Wipe Info-Slack Space only (Windows 98/Me)	Wipes the empty, or slack, disk space that was formerly occupied by the selected item. See "Wipe files or folders" on page 251.
Wipe Info-Wipe Free space (Windows 98/Me)	Wipes the empty disk space that is related to the selected item. See "Wipe files or folders" on page 251. See "To wipe free space in Windows 2000/XP" on page 251.

Start utilities from the CD

You can start Norton Disk Doctor, Norton WinDoctor, Wipe Info, and Fast & Safe Cleanup from the CD. In Windows 98, you can also start UnErase Wizard.

To start utilities from the CD

1 Insert the CD into the CD-ROM drive.

2 In the CD window, click **Launch Utilities from CD**.

3 In the CD Utilities window, select a utility. Your options are:

Norton Disk Doctor	See "To run Norton Disk Doctor from the CD" on page 20. See "Check your disk with Norton Disk Doctor" on page 206.
Norton WinDoctor	See "Find and fix Windows problems" on page 210.
Wipe Info	See "Eliminating data permanently" on page 247.
UnErase Wizard (Windows 98/Me)	See "Recovering missing or erased files" on page 219.
Fast & Safe	See "Removing unwanted files and programs" on page 257.

4 Run the utility.
For more information, refer to the instructions for the utility that you want to run.

5 When you have finished running the utility, close it.

6 In the CD Utilities window, click **Exit**.

7 Close the CD window.

Access Extra Features

Norton SystemWorks Extra Features include additional software and Internet-based services to enhance your computing security and productivity. These include Symantec Web features, Tech24.com and Symantec Security Check, and other programs. You can access Extra Features from the main window. To access some features, you must have an active Internet connection.

To access Extra Features

1 On the left side of the main window, click **Extra Features**, then select a feature. Your options are:

Symantec Web	Connects you to Web sites where you can run the following Web-based programs: ■ Symantec Security Check examines your computer for conditions that make it vulnerable to threats, intrusions, or identity theft ■ Tech24 accesses Web-based technical support
Process Viewer	Displays all programs that are currently running on your computer
PerformanceTest	Compares your computer's performance with other selected systems, using a variety of tests

2 Follow the on-screen instructions to run the selected program.

Start Norton AntiVirus

After installation, Norton AntiVirus automatically protects any computer on which it is installed. You do not have to start the program to be protected.

To start Norton AntiVirus

❖ Do one of the following:

- On the Windows taskbar, click **Start** > **Programs** > **Norton SystemWorks** > **Norton AntiVirus** > **Norton AntiVirus**.
- On the Windows XP taskbar, click **Start** > **More Programs** > **Norton SystemWorks** > **Norton AntiVirus** > **Norton AntiVirus**.
- On the desktop, double-click the Norton SystemWorks Professional icon.

Use the Norton AntiVirus icon in the Windows system tray

See "Customize Norton AntiVirus" on page 120.

Norton AntiVirus adds an icon to the Windows system tray at the end of the Windows taskbar. Use the icon in the Windows system tray to open Norton AntiVirus and to enable or disable Auto-Protect.

To use the Norton AntiVirus Windows system tray icon

❖ In the Windows system tray, right-click the Norton AntiVirus icon, then on the tray icon menu, select the option that you want.

Use the Windows Explorer toolbar

Norton AntiVirus adds a button and menu to Windows Explorer.

When you first open Windows Explorer after installing Norton AntiVirus, you may not see the Norton AntiVirus button and menu. You might have to restart Windows before the toolbar button appears.

You may not be able to access the Norton AntiVirus Windows Explorer menu, depending on your computer's configuration.

To display the Norton AntiVirus button and menu

1 In Windows Explorer, on the View menu, click **Toolbars** > **Norton AntiVirus**.

2 Click the arrow to the right of the button to view your options. Your options are:

View Status	Launches Norton AntiVirus and displays the Status window with system status. See "Check Norton AntiVirus configuration status" on page 82.
View Quarantine	Displays the Quarantine area and the files currently stored there. See "If Norton AntiVirus places files in Quarantine" on page 196.
View Activity Log	Displays the Log Viewer, which shows you various Norton AntiVirus activities, such as scans performed and problems found. See "Monitor Norton AntiVirus activities" on page 84.
View Virus Encyclopedia	Connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.
Launch Scan Menu	Opens Norton AntiVirus in the Scan for Viruses pane, on which you can specify a scan to run.

Disable or enable Smart Sweep/Internet Sweep

The Norton CleanSweep tool Smart Sweep/Internet Sweep monitors your computer for new program installations and Internet downloads. Smart Sweep/Internet Sweep records where new programs are installed. This information is used by other Norton CleanSweep tools, including Backup Wizard, Uninstall Wizard and Internet Uninstall Wizard.

When Norton SystemWorks is installed in Windows 98/Me, Smart Sweep/Internet Sweep is configured to start with Windows. When Norton SystemWorks is installed in Windows 2000/XP, Smart Sweep/Internet Sweep is not configured to start with Windows.

If you do not install or remove programs frequently, you do not need to have Smart Sweep/Internet Sweep start with Windows.

To change Smart Sweep and Internet Sweep startup options

1. On the Options menu, click **Norton CleanSweep**.
2. In the Options dialog box, click **Smart Sweep/Internet Sweep**.
   On the Smart Sweep/Internet Sweep tab, the Smart Sweep/Internet Sweep status indicates that it is currently active or not active.
3. Do one of the following:
   - (Windows 98/Me) Select **Turn Smart Sweep/Internet Sweep on**.
   - (Windows 98/Me) Select **Turn Smart Sweep/Internet Sweep off**.
   - (Windows 2000/XP) Check or uncheck **Load Smart Sweep/Internet Sweep on Startup**.
4. Click **OK**.

If Smart Sweep/Internet Sweep has started with Windows, two icons appear in the Windows system tray, (Norton Tray Manager in some versions of Windows).

Use these icons to temporarily disable Smart Sweep/ Internet Sweep.

To temporarily disable Smart Sweep/Internet Sweep

1. On the Windows desktop, move the mouse pointer over the Windows system tray area.

   See "Use Norton Tray Manager" on page 67.

   If Norton Tray Manager is active, you might have to open it first to see the Smart Sweep/Internet Sweep icons.
2. Do one of the following:
   - Right-click the Smart Sweep icon, then click **Close**.
   - Right-click the Internet Sweep icon, then click **Close**.
3. In response to the confirmation message, click **Yes**.

Disable or enable Norton System Doctor

If you want to perform tasks on your computer that require that no other applications are running, you can prevent Norton System Doctor from starting with Windows.

To disable or enable Norton System Doctor

1. On the Options menu, click **Norton Utilities**.
2. In the Norton Utilities Options dialog box, click **Startup Programs**.
3. On the Startup Programs tab, under Current User, check or uncheck **Norton System Doctor**.
4. If you share your computer with others and want Norton System Doctor to start whenever any user logs on, under All Users, ensure that **Norton System Doctor** is checked.
5. Click **OK**.

Temporarily disable Auto-Protect

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses, Trojan horses, worms, and other malicious threats. It checks programs for viruses as they are run and monitors your computer and removable media for any activity that might indicate the presence of a virus. When a virus or virus-like activity is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect.

If you have set a password for Options, Norton AntiVirus asks you for the password before you can view or adjust the settings.

To temporarily disable Auto-Protect

See "Start Norton AntiVirus" on page 71.

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Auto-Protect**.
3. In the Auto-Protect pane, uncheck **Enable Auto-Protect**.

Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

To enable Auto-Protect

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Auto-Protect**.
3. In the Auto-Protect pane, check **Enable Auto-Protect**.

If the Norton AntiVirus icon appears in the Windows system tray, you can use it to enable and disable Auto-Protect.

To enable or disable Auto-Protect using the icon in the Windows system tray

❖ In the Windows system tray, right-click the Norton AntiVirus icon, then do one of the following:

- If Auto-Protect is disabled, click **Enable Auto-Protect**.
- If Auto-Protect is enabled, click **Disable Auto-Protect**.

Disable Norton Password Manager monitoring

You can disable Norton Password Manager monitoring of Web browsers and Windows programs. When these features are turned off, Norton Password Manager does not react when you open Web sites or Windows programs that require you to sign in. When these features are turned on, Norton Password Manager displays a dialog box when you open programs or Web sites that require you to sign in.

Any changes to Web and Windows program monitoring apply to the current profile.

To disable Web browser or Windows program monitoring

1. On the left side of the main window, click **Password Manager** > **Status & Settings**.
2. In the Status and Settings pane, under Monitoring Status, select one of the following:
   - Web Browser
   - Windows Programs
3. On the right side of the window, click **Off**.

Perform a One Button Checkup

One Button Checkup scans your computer with a collection of diagnostic tools that cover the most critical computer activities, such as virus protection and disk integrity.

You can run One Button Checkup whenever you think that you may have a problem, and to ensure that your computer is performing to its optimum capability. You can customize One Button Checkup to specify which scans should run, and schedule automatic checkups. You can also view a history of repairs that were made by One Button Checkup, and undo a repair if necessary.
See "Norton SystemWorks options" on page 100.

One Button Checkup includes selected tools from Norton Utilities, Norton AntiVirus, and Web Cleanup.

Norton SystemWorks component	**One Button Checkup scans**
Norton Utilities	■ Registry Doctor (Windows 98/Me) ■ WinDoctor: Windows Registry Scan, Program Integrity Scan, and Shortcut Scan ■ Norton Optimization Wizard: Registry Integrity Scan (Windows 98/Me) ■ Speed Disk: Disk Fragmentation Scan (Windows 98/Me) ■ Norton Disk Doctor: Disk Integrity Scan (Windows 98/Me)
Norton AntiVirus	■ Virus Definitions Check ■ Auto-Protect Check ■ Last Virus Scan Check
Web Tools	■ Web Cleanup: Web Cleanup Scan

To perform a One Button Checkup

1. In the main window, click **One Button Checkup** > **Begin Checkup**.
   One Button Checkup starts to run its diagnostic scans.
2. If you need to interrupt the checkup, click **Stop Scan**.
   When the scans are complete, One Button Checkup displays a summary of scan results that are grouped by scan category.
3. Select the action that you want to take. Your options are:

View error details before One Button Checkup repairs them.	See "To view details after a One Button Checkup" on page 79.
Exclude an error from repair.	See "To ignore problems that were found by One Button Checkup" on page 80.

4. To let One Button Checkup proceed with repairs, click **Begin Fix**.
   If One Button Checkup can't fix a problem, it prompts you to use another program to fix the problem manually.
5. After you have repaired the problems, click **Rescan** to ensure that all of the problems are fixed.
6. When the repairs are complete, in the One Button Checkup scan summary dialog box, click **Close**.

If you do not want to have all of the problems repaired automatically, you can view their details and select which problems to fix.

To view details after a One Button Checkup

1. Perform a One Button Checkup.
2. In the Scan complete dialog box, next to the scan that you want to view, click **view details**.
   A more detailed description of the problem appears below the scan name.

Ignore problems found by One Button Checkup

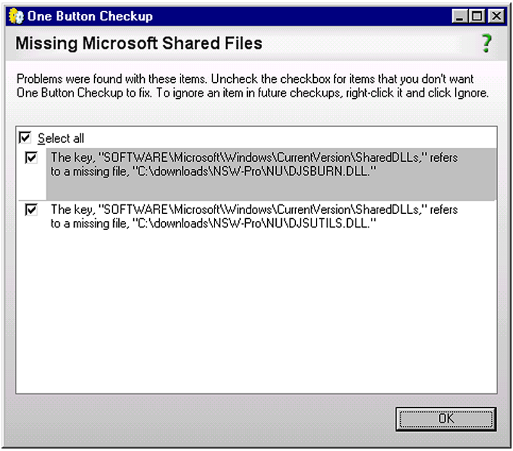
You can have One Button Checkup ignore selected problems on future scans. The problem is added to an Ignore Problems list. You can also remove a problem from the Ignore Problems list.

To ignore problems that were found by One Button Checkup

See "Perform a One Button Checkup" on page 78.

1 Perform a One Button Checkup.

2 In the Scan complete dialog box, next to a reported error, click **view details**.



Problems were found with these items. Uncheck the checkbox for items that you don't want One Button Checkup to fix. To ignore an item in future checkups, right-click it and click Ignore.

☑ Select all

☑ The key, "SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs," refers to a missing file, "C:\downloads\NSW-Pro\NU\DJSBURN.DLL."

☑ The key, "SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs," refers to a missing file, "C:\downloads\NSW-Pro\NU\DJSUTILS.DLL."

3 Do one of the following:

- If you don't want One Button Checkup to find any problems of this category for this scan, uncheck the item.
- If you want One Button Checkup to ignore a specific problem for this one time only, open the Problem Details dialog box and uncheck it.
- If you want One Button Checkup to ignore a specific problem until you indicate otherwise, open the Problem Details dialog box, right-click the item, then click **Ignore Selected Problem**.

You can view previous One Button Checkup repairs and undo repairs, if necessary. You might undo a repair if, for example, One Button Checkup deleted an expected shortcut file and you want to restore it. Repairs that are performed in a One Button Checkup are grouped chronologically by session.

To view the One Button Checkup Repair History or to undo repairs

1. In the main window, click **One Button Checkup**.
2. In the bottom right of the One Button Checkup window, click **Repair History**.
3. In the Repair History window, select the date for the repairs that you want to view.
4. Do one of the following:
   - Click **View Details** to see the specific tasks and changes that One Button Checkup made during the checkup.
   - Click **Export History** to export a text description of all of the history repairs for all of the repair dates.
     You will be prompted to specify a name for the exported text file. Check one or more repair descriptions.
   - Check **Select all** to select all of the repairs in a single One Button Checkup session.
5. Click **Undo** to undo a selected repair.
   One Button Checkup restores the problem condition to the state that it was in before the repair. You might have to restart your computer for some reversed repairs to take effect.
6. Click **Close**.

Check Norton AntiVirus configuration status

If Norton AntiVirus is behaving in an unexpected way, or if you're not sure that everything is being scanned for viruses, check the status on the main window.

In the System Status pane of the Norton AntiVirus main window, a check mark indicates that the system status is OK and a triangle indicates that your system needs attention. If you see a triangle, review the features to see which area needs attention.

If you see an exclamation point, it indicates that your subscription is either expired or your virus definitions are more than two weeks old. If your subscription is expired, renew it to maintain your protection. If your subscription is current, then you need to update your virus definitions.

See "Customize Norton AntiVirus" on page 120.

If you need to adjust any settings, use Options.

To check system status

1. In the main window, under Norton AntiVirus, click **Status**.
2. In the System Status pane, review the status to the right of each feature.
3. For information about a particular feature, select the feature.
   The right pane displays a description and a link to more information about the feature.

Check Office Plug-in status

Office Plug-in protects Microsoft Office documents from viruses, worms, and virus-like activities. It scans documents whenever you open them in a Microsoft Office program. Office Plug-in is enabled in Options.

If you have set a password for Options, Norton AntiVirus asks you for the password before you can view or adjust the settings.

To check Office Plug-in status

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the left pane of the Options window, under Other, click **Miscellaneous**.
3. Verify that Office Plug-in is enabled.

Monitor Norton AntiVirus activities

Occasionally, you may need to look at previous Norton AntiVirus activities, such as when the last system scan was done or how many viruses were detected last week. Norton AntiVirus displays a record of its threat detection, application, and error activities in the Log Viewer.

About the Log Viewer

The Log Viewer displays the history of activities in each Activity Log. An Activity Log is a collection of multiple log files, one for each type of information collected: threat alerts, application activities, and errors.

Using the information in the Log Viewer, you can:

- View detailed information recorded in each log by selecting the log in the left column and viewing the the details in the right pane.
- Delete the activity entries for a log by selecting the log, then clicking Clear. If you never clear the entries for a category, it expands until it reaches the maximum size. Then it starts overwriting the oldest entries.

Check the Activity Log

Check the Activity Log to see what tasks were performed and the results of those tasks to make sure that your Options settings are appropriate for your particular needs.

To check the Activity Log

1. In the main window, under Norton AntiVirus, click **Reports**.
2. In the Reports pane, on the Activity Log line, click **View Report**.

3 In the left pane, select the log that you want to review. Your options are:

Threat alerts	A history of threat alerts, such as the ID and type of threat, date and time when it occurred, the action taken, and the version of the virus definitions used.
Application activities	A history of scanning activities, such as when scanning occurred and with what results.
Errors	Detailed information about any problems encountered when scanning your computer such as the date, error code, and message.

As you select each log, the right pane changes and displays details specific to the particular log. The most recent activities appear at the top of the log.

4 When you are finished viewing the information, click **File** > **Exit**.

Create and use Rescue Disks

Rescue Disks are available only for Windows 98/Me.

Rescue Disks are images on floppy disks that let you restart your computer when your hard disk is damaged or infected with a virus.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue utilities, configuration files, and a DOS-based Norton AntiVirus scanner across multiple floppy disks or on a network drive.

You can customize your Rescue Disk set. It can consist of one *bootable* floppy disk, one Norton AntiVirus Program floppy disk, and at least six Virus Definition floppy disks. If you have Norton Utilities installed, you can also have two Norton Utilities floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.

Rescue Disks contain information specific to the computer on which they were made.

If you are using Rescue Disks for recovery, you must use the disks made for your computer.

If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer.

See "If you need to use Rescue Disks to restore your system" on page 91.

You should update Rescue Disks whenever you update your virus protection, install new software, or make changes to your hardware.

Create a Rescue Disk set

You can create Rescue Disks any time. You can start the Rescue Disk Wizard from the main window of your Symantec product.

If you start the Rescue Disk Wizard from the main window, temporarily disable Auto-Protect while you are creating the Rescue Disk set. If you do not restart your computer after creating Rescue Disks, remember to enable Auto-Protect again.

When you select a floppy disk drive, the Rescue Disk program calculates the number of disks that you will need to complete the set. Depending on what items you want to include in the Rescue Disk set, you might need ten or more floppy disks.

If you choose to create Rescue Disks on a network drive, a second physical hard disk, or some other large capacity disk drive (but not a CD), your Rescue Disk set is placed in a folder on the selected disk. Make sure that you also have a bootable floppy disk in a safe location. This disk should contain the network *drivers* or other files necessary to start your computer and access the drive on which you placed your Rescue Disk set. Creating a Rescue Disk set on a startup hard disk, for example, drive C, is not recommended because you will not be able to access the rescue programs and configuration files if your hard disk is damaged and unable to start.

To create Rescue Disks

1 In the main window, click **Rescue**.

2 In the Rescue Disk window, select the drive on which to create the Rescue Disk set.
To create a Rescue Disk set on floppy disks, select drive A.
When you select a floppy disk drive, the Basic Rescue program displays the number of floppy disks that you will need to create the Rescue Disk set.

3 To make changes to the default Rescue Disk settings, click **Options** and do the following:
   - On the Rescue Files tab, specify the files to include in the Rescue Disk set. If you change the default file selection, the number of required floppy disks will also change.
   - On the Format Settings tab, select the type of format, if any, that you want Rescue Disk to use when it prepares the bootable floppy disk for the Rescue Disk set.

4 Click **OK** to return to the Rescue Disk window.

5 When you have either assembled the required number of floppy disks or identified another location for the Rescue Disk files, click **Create**.
If you selected a floppy disk drive, Rescue Disk displays the Basic Rescue Disk List window and an estimate of how much time you will need to create the entire set.

6 Label the disks as specified in the Basic Rescue Disk List window, or type a descriptive name, then click **OK**.
Rescue Disk prompts you to insert the first disk in the floppy disk drive. If you selected a network drive or other larger-format drive, Rescue Disk prompts you for a Rescue Folder drive location.

7 Insert the disks as requested.

8 When you have finished creating the basic Rescue Disk set, in the Rescue Disk window, click **Close**.

Test your Rescue Disks

After you have created the Rescue Disk set, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.

If you created Rescue Disks on a network drive, a second physical hard disk, or some other large capacity disk drive, you will have to restart into DOS from an external floppy disk, navigate to the Rescue folder, and run Rescue.exe.

To test your Rescue Disks

1 Close all open Windows programs.

See "My Rescue Disk does not work" on page 301.

2 Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.
If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly.
If the Rescue Disk screen does not appear, you have several options for correcting the problem.

3 Press **Escape** to exit to DOS.

4 Remove the disk from drive A and slide open the plastic tab on the back of the disk to write-protect it.

5 Restart your computer.

Update your Rescue Disks

You can update your Rescue Disks as often as you like. Rescue Disk lets you update your basic Rescue Disk set without having to recreate them.

If you are updating a floppy disk set, make sure that your disks are not write-protected before you begin.

To update your Rescue Disks

1 In the main window, click **Rescue**.

2 In the Rescue Disk window, under Select Destination Drive, click **drive A**, then click **Update**.
A message prompts you to insert the disk labeled Basic Rescue Boot Floppy Disk into drive A.

3. Insert the Basic Rescue Boot Floppy Disk into drive A, then click **OK**.
4. Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted.

See “Test your Rescue Disks” on page 89.

Rescue Disk options

Rescue Disk has the following options.

Add Files	Click to specify additional files that you want Rescue Disk to store on the Rescue Disk set. ⚠ Do not use this as a backup utility. Add files only if they are needed to restore your system after a crash.
Remove File	Click to remove the selected file under User-selected Files. The files will no longer be included on the Rescue Disk set.
Rescue items list	The list is categorized and presented in a hierarchical view, similar to a Windows Explorer view. Click the plus sign next to a category to expand the list and see what the category contains. Click the plus sign next to a specific file for more information about the file. The list of rescue items is different depending on the programs you have installed and the type of Rescue Disk set you are using.
Basic Rescue Boot Floppy Files	Files that Rescue Disk stores on the floppy disk that you use to start your system.
Rescue DOS Utility Programs	DOS-based emergency programs that Rescue Disk stores on the Rescue Disk set. You can use these DOS-based utilities to recover your system.
Norton AntiVirus Program	Norton AntiVirus program files.

Definitions Disks	Virus definitions files used by Norton AntiVirus to scan your system in an emergency. There are several of these disks.
User-selected Files	Files you have added to the Rescue Disk set. Add files to this list by clicking Add Files. Remove files from this list by clicking the file, then clicking Remove File.

If you need to use Rescue Disks to restore your system

Rescue Disks are available only for Windows 98/Me.

Sometimes a virus or threat prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus *alert* tells you when to use your Rescue Disks.

You first need to determine if your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you did any of the following:

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions
- Upgraded your operating system
- Updated virus definitions

If your Rescue Disks are not current, you can still use them to remove viruses from your computer. When the Rescue Disk screen appears, use only the Norton AntiVirus task.

To use your Rescue Disks

1. Insert the Basic Rescue Boot Floppy Disk into drive A and restart your computer.
   The Rescue program runs in DOS.
2. Use the arrow keys to select the program that you want to run.
   A description of the selected program appears in the right pane of the Rescue program. Your options are:

Norton AntiVirus	Scans your computer for viruses and repairs any infected files
Rescue Recovery	Checks and restores boot and partition information

3. Press **Enter** to run the selected program.
4. Follow the on-screen instructions for inserting and removing the Rescue Disks.
5. When the Rescue program is done, remove the Rescue Disk from drive A and restart your computer.

For more information

The product documentation provides glossary terms, online Help, a Readme file, the User's Guide in PDF format, and links to the Knowledge Base on the Symantec Web site.

Look up glossary terms

Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. In both locations, clicking a glossary term takes you to its definition.

Use online Help

Help is available throughout your Symantec product. Help buttons or links to more information provide information that is specific to the task that you are completing. The Help menu provides a comprehensive guide to all of the product features and tasks that you can complete.

To use online Help

1 At the top of the main window, click **Help & Support** > **Norton SystemWorks Professional**.

2 In the Help window, in the left pane, select a tab. Your options are:

Contents	Displays the Help by topic
Index	Lists Help topics in alphabetical order by key word
Search	Opens a search field in which you can enter a word or phrase

Window and dialog box Help

Window and dialog box Help provides information about the program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

❖ Do one of the following:
  - In the window, click any available Help link.
  - In the dialog box, click **Help**.

View Norton Ghost Help

Norton Ghost has an extensive online Help system that describes how to use all of its features.

To view Norton Ghost Help

❖ At the top of the main window, click **Help & Support** > **Norton Ghost Help**.

Readme file

The Readme file contains information about installation and compatibility issues. It also contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the product files.

To read the Readme file

1. In Windows Explorer, double-click **My Computer**.
2. Double-click the hard disk on which you installed Norton SystemWorks Professional.
   In most cases, this will be drive C.
3. Click **Program Files** > **Norton SystemWorks Professional**.
4. Double-click **Readme.txt**.
   The file opens in Notepad or your default word processing program.
5. Close the word processing program when you are done reading the file.

Access the User’s Guide PDF

The *Norton SystemWorks Professional User’s Guide* is provided on the CD in PDF format. You must have Adobe

Acrobat Reader installed on your computer to read the PDF.

If you purchased this product as an electronic download, Adobe Acrobat Reader was not included. You must download it from the Adobe Web site.

A PDF of the *Norton Ghost User's Guide* is also on the CD.

To install Adobe Acrobat Reader

1. Insert the CD into the CD-ROM drive.
2. Click **Browse CD**.
3. In the CD window, double-click the **Manual** folder.
4. Double-click the **Acrobat** folder.
5. Double-click the program file.
6. Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.

If you do not have a CD, you can download the PDF from the Symantec Service & Support Web site.

To read the User's Guide PDF from the CD

1. Insert the CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Do one of the following:
   - Double-click **NSWP2004.pdf** to open the *Norton SystemWorks Professional User's Guide*.
   - Double-click **Manual.pdf** to open the *Norton Ghost User's Guide*.

You can also copy a User's Guide to your hard disk and read it from there.

To read a User's Guide from your hard disk

1. Open the location into which you copied the PDF.
2. Double-click the PDF.

Symantec products on the Web

The Symantec Web site provides extensive information about all Symantec products. There are several ways to access the Symantec Web site.

To access the Web site from the Help menu

❖ Select the solution that you want. Your options are:

Symantec Security Response	Takes you to the Security Response page of the Symantec Web site, from which you can update your protection and read the latest information about antithreat technology.
More Symantec solutions	Takes you to the Symantec Store Web site, from which you can get product information on every Symantec product.

Within your Symantec product, the Reports page contains a link to the Symantec online Virus Encyclopedia, as does the Windows Explorer toolbar.

To access the Web site from the Reports page

1. In the main window, under Norton AntiVirus, click **Reports**.
2. On the Reports page, next to Online Virus Encyclopedia, click **View Report**.

To access the Symantec Web site from Windows Explorer

1. Open Windows Explorer.
2. On the toolbar, on the Norton AntiVirus menu, click **View Virus Encyclopedia**.
   This option connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.

To access the Symantec Web site in your browser

❖ On the Internet, go to www.symantec.com

Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special *virus definitions* releases.

To subscribe to the Symantec Security Response newsletter

1. On the Internet, go to securityresponse.symantec.com
2. On the security response Web page, scroll down to the reference area of the page, then click **Newsletter**.
3. On the security response newsletter Web page, select the language in which you want to receive the newsletter.
4. On the subscribe Web page, type the information requested, then click **Subscribe**.

Options

5

The default settings for this product provide complete protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply. You can change the product's settings to fit your work environment.

If you are using Windows 2000/XP, you will need administrator access to change options. If you are an administrator and share your computer with others, keep in mind that the changes that you make apply to everyone using the computer.

Norton SystemWorks options

Norton SystemWorks includes a collection of programs that can be customized to suit your computing needs. Some general options are accessible from the main window. Many other options are only accessible from within specific programs. Start the program to locate and customize the available options for that program.

Customize One Button Checkup Repair History

You can view a record of repairs, export a report of the repairs performed during a One Button Checkup scan, select and undo specific repairs, and specify how long to retain a record of One Button Checkup repairs in One Button Checkup Advanced Options.

To set One Button Checkup Repair History options

1. In the bottom right of the main window, click **Options**.
2. In the Norton SystemWorks Options dialog box, on the One Button Checkup tab, click **Advanced Options**.
3. In the One Button Checkup Advanced Options dialog box, on the Repair History tab, select the duration for the repair history. Your options are:

Days	Type the number of days.
Number of repairs	Type the number of repairs to be logged before One Button Checkup deletes the Repair History.
Forever	Click Forever if you want to keep a record of all of the repairs.

4. Do one of the following:
   - To view the history of a previous One Button Checkup repair, click **View History**.
     See "Customize One Button Checkup Repair History" on page 100.
   - To clear all of the Repair History, click **Clear History**.
5. Click **OK** to close the One Button Checkup Advanced Options dialog box.
6. Click **OK** to close the Norton SystemWorks Options dialog box.

Create a new One Button Checkup schedule

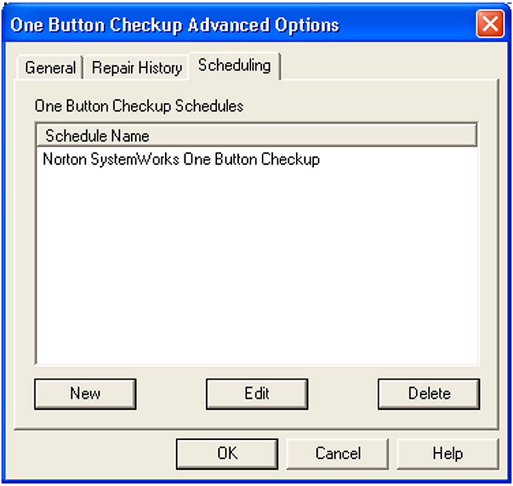
When Norton SystemWorks is installed, One Button Checkup is scheduled to run its full set of scans on Fridays at 5:30 P.M. If One Button Checkup finds any errors, it prompts you to fix them. You can set One Button Checkup schedule options to run specific scans and to repair any problems automatically.

You can use the One Button Checkup Schedule wizard to assist you in creating a customized schedule. You can set the date and time, include or omit specific scans, and assign a name for the scan.

In Windows 2000/XP, you must have *Administrator access rights* to schedule a One Button Checkup.

To create a new One Button Checkup schedule

1 In the bottom right of the main window, click **Scheduling**.



Norton SystemWorks One Button Checkup

2 In the One Button Checkup Advanced Options dialog box, on the Scheduling tab, click **New**.

3 In the Schedule wizard, click **Next**.

4 In Windows 2000/XP, type your Windows logon ID and password.
One Button Checkup Scheduler needs this information in order to run on schedule automatically.

5 Do the following:

- Type a name for the schedule. This name appears in the Scheduling list.
- If you want problems to be repaired automatically during scheduled scans, check **Auto repair during scheduled One Button Checkup scans**. If this is unchecked, One Button Checkup will not repair problems automatically.

6 Click **Next**.

7 In the Customize Scanners list, specify the scans that you want to run as part of this scheduled checkup, then click **Finish**.
See "About One Button Checkup scan options" on page 110.
The new scan is set to run on Fridays at 5:30 p.m. You can change the time and set other scheduling options by editing the schedule.
See "Change a One Button Checkup schedule" on page 103.

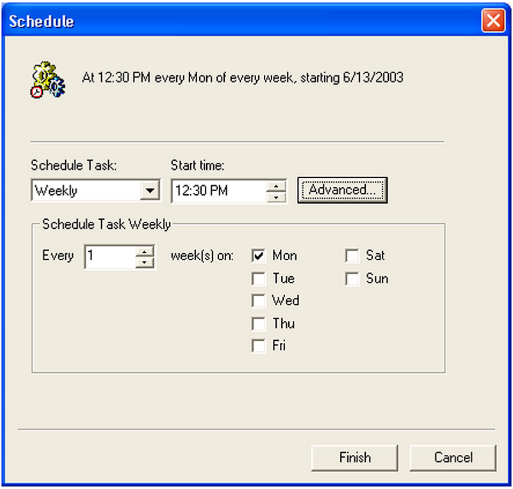
Change a One Button Checkup schedule

If you want to change an existing One Button Checkup schedule, you can change the time and day, the frequency, and the specific scans that occur as part of the schedule.

To edit an existing One Button Checkup schedule

1 On the lower right of the main window, click **Scheduling**.

2 In the One Button Checkup Advanced Options dialog box, on the Scheduling tab, select a scheduled scan, then click **Edit**.



At 12:30 PM every Mon of every week, starting 6/13/2003

Schedule Task: Weekly

Start time: 12:30 PM

Schedule Task Weekly

Every 1 week(s) on: ☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

3 In the selected schedule's dialog box, in the Schedule Task list, select the time that you want the scheduled scan to run. Your options are:

Daily	Specify the number of days between checkups.
Weekly	Specify a weekly interval and days of the week.
Monthly	Specify the months in which you want to scan and the day of the month.
Once	Specify any day of the year.
At System Startup	Run One Button Checkup every time that Windows starts.

At Logon	Run One Button Checkup every time that you log on to Windows.
When idle	Run One Button Checkup after the computer has been idle for the specified number of minutes.

4. Specify a Start time if that option is available.
   Some scheduled tasks have automatic start times.
5. To configure multiple versions of the selected schedule, check **Show multiple schedules**.
6. Click **New** to add a duplicate of the current schedule.
   You can change the settings for this duplicate.
7. Click **Advanced** to specify start and end dates for the scheduled scans, or to have the activity repeat on an hourly or daily basis.
   See "Set One Button Checkup Advanced Schedule options" on page 106.
8. On the Customize tab, uncheck the scans that you don't want to run as part of this schedule.
   See "About One Button Checkup scan options" on page 110.

   If you normally logon to your computer, you might need to type your logon password before you can save the schedule.
9. Click **OK** to close the Norton SystemWorks Options dialog box.

If you choose to ignore any errors while using Norton WinDoctor, One Button Checkup may still report these errors during its scan and suggest that you run Norton WinDoctor again. One Button Checkup and Norton WinDoctor do not share the same settings, so you will have to fix these errors using Norton WinDoctor to stop this message from displaying.

Set One Button Checkup Advanced Schedule options

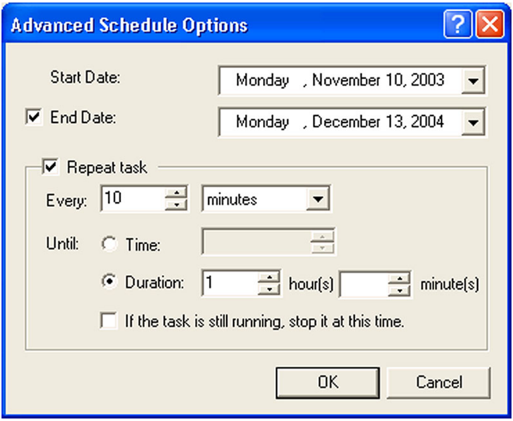
In One Button Checkup you can specify start and end dates for scheduled scans, repeat the scan on an hourly or daily basis, or have the scan stop after a specified duration.

To set One Button Checkup Advanced Schedule options

1 On the lower right of the main window, click **Scheduling**.

2 In the One Button Checkup Advanced Options dialog box, on the Scheduling tab, select a scheduled scan, then click **Edit**.

3 In the selected schedule's dialog box, click **Advanced**.



Start Date: Monday , November 10, 2003

☑ End Date: Monday , December 13, 2004

☑ Repeat task

Every: 10 minutes

Until: ○ Time:

● Duration: 1 hour(s) minute(s)

□ If the task is still running, stop it at this time.

4 In the Advanced Schedule Options dialog box, specify a Start Date, and whether you want to repeat the task for a specified time. Your options are:

Start Date	On the calendar list, select the date that the schedule should start.
End Date	On the calendar list, select the date that the schedule should end.
Repeat task	Specify a frequency for the task, in hours or minutes.
Time Duration	Specify a time or the number of hours and minutes that should elapse before the schedule stops.

5 Check or uncheck **If the task is still running, stop it at this time**.

6 Click **OK** to close the Advanced Schedule Options dialog box.

7 In the selected schedule's dialog box, make any other changes to the schedule and the scans that will run during this schedule.
See "Change a One Button Checkup schedule" on page 103.

Set One Button Checkup Repair History options

You can specify how long to retain a record of One Button Checkup repairs in One Button Checkup Advanced Options.

To set One Button Checkup Repair History options

1 In the One Button Checkup Details pane, click **Options**.

2 Click **Advanced Options**.

3 On the Repair History tab, indicate the duration for the Repair History. Your options are:

Days	Type the number of days.
Number of Repairs	Type the number of repairs before One Button Checkup deletes the history.
Forever	Click Forever if you want to keep a record of all repairs.

4 To view the history of a previous One Button Checkup repair, click **View History**.
See "Customize One Button Checkup Repair History" on page 100.

5 When you've made your selections, click **OK**.

Set Norton SystemWorks options

The default settings for Norton SystemWorks provide a safe, automatic, and efficient way of protecting your computer and maintaining its performance. On the Options menu in the Norton SystemWorks main window, you can access options for Web Tools, One Button Checkup, Norton AntiVirus, Norton Utilities, and Norton CleanSweep.

You change Norton SystemWorks general settings on the tabs in the Norton SystemWorks Options dialog box.

To set Norton SystemWorks general options

1 On the Options menu, click **Norton SystemWorks**.

2 In the Norton SystemWorks Options dialog box, click a tab.

3 On the selected tab, set the options that you want. Your options are:

Startup	See "About Startup options" on page 109.
General	See "About General options" on page 110.
One Button Checkup	See "About One Button Checkup scan options" on page 110.
One Button Checkup Advanced Options	See "About One Button Checkup Advanced options" on page 111.

About Startup options

Norton SystemWorks Startup options let you select programs to start when Windows starts. When they are checked, the following Norton SystemWorks programs start with Windows:

Norton AntiVirus Auto-Protect	Remains in memory and monitors your computer for any signs of virus threats.
Fast & Safe Cleanup	Cleans temporary files from your hard disks.
Smart Sweep/ Internet Sweep	Automatically monitors program installations, including programs that are downloaded from the Internet.
Norton Disk Doctor	Examines your hard disks for errors.
Norton System Doctor	Remains in memory and monitors your computer for selected conditions.

About General options

General options let you specify whether splash screens and program introductions should appear when Norton SystemWorks programs start and whether you receive critical updates. General options include the following:

Display program splash screens	Displays the graphic window for each program when the program is started. Uncheck to bypass the graphic and open the program's main window.
Display program introduction dialogs	Displays a brief description of the program every time you start the program.
Norton Tray Manager (Windows 98/Me/2000)	Collects the taskbar icons for memory-resident Norton SystemWorks programs into one icon.
Disable Critical Update Notification and system-wide Automatic LiveUpdate	Disables Automatic LiveUpdate and prevents LiveUpdate from notifying you if critical program updates are available.

About One Button Checkup scan options

See "Create a new One Button Checkup schedule" on page 101.

Before you run One Button Checkup, you can select which scans are included. For example, if you have already scheduled a regular Norton AntiVirus scan, you could disable it in One Button Checkup options. One Button Checkup scans include the following:

Registry Doctor (Windows 98/Me)	Checks for problems with the registry that might cause computer problems.
Windows Registry Scan	Checks for inaccurate and obsolete entries in the Windows registry that could cause errors.

Program Integrity Scan	Ensures that a program's associated files are in their expected locations, and helps you locate them if they are missing.
Virus Definitions Check	Checks that your virus definitions are up-to-date so that you are protected against the latest virus threats.
Auto-Protect Check	Verifies that Auto-Protect is enabled and working in the background to protect your computer from virus threats.
Last Virus Scan Check	Checks the date on which Norton AntiVirus performed a complete scan of your computer's hard disks to ensure that your disks are virus-free.
Shortcut Scan	Checks for mismatched or missing program and file shortcuts and helps you locate them.
Disk Integrity (Windows 98/Me)	Checks that your local hard disks are not showing any signs of hardware failure.
Disk Fragmentation (Windows 98/Me)	Checks the level of fragmentation on your local hard disks and starts Speed Disk if the fragmentation level is too high.
Web Cleanup Scan	Checks for the number of Internet files, cookies, and history that can be deleted by Web Cleanup.

About One Button Checkup Advanced options

The One Button Checkup Advanced Options dialog box has the following three tabs that let you manage ignored problems, previous repairs, and future scheduling:

General	Lets One Button Checkup check for problems that you previously indicated should be ignored. See "Ignore problems found by One Button Checkup" on page 80.

Repair History	Lets you specify how long to keep a record of One Button Checkup repairs. See "Customize One Button Checkup Repair History" on page 100.
Scheduling	Lets you schedule automatic One Button Checkups. See "Create a new One Button Checkup schedule" on page 101.

Set Norton Utilities options

The Norton Utilities options let you control the display of introductory messages, the utilities that should start with Windows, and the behavior of the Windows Recycle Bin if Norton Protection is enabled.

To set Norton Utilities options

1. On the Options menu, click **Norton Utilities**.
2. Specify the settings. Your options are:

General Settings	Control the display of splash screens and introductory information.
Startup Programs	Set the Norton Utilities applications (Norton Disk Doctor and Norton System Doctor) that start with Windows.

Recycle Bin	Specify the behavior of the Recycle Bin when you double-click it. You can set this option to open UnErase Wizard, recently deleted files (Windows 98/Me), all protected files, or the standard Windows Recycle Bin. You can also rename the Norton Protected Recycle Bin.
Norton Protection	Customize settings for Norton Protection, including which disks are protected, which file types should be automatically included or excluded from protection, and how long deleted files should be protected.

3 Click **OK**.

Set Norton System Doctor startup options

Norton System Doctor continuously monitors your computer to keep it free of problems and running at peak efficiency. It can alert you when conditions require attention, and fix many problems automatically, without interrupting your work.

To take full advantage of Norton System Doctor monitoring capabilities, leave it running at all times. You can also specify whether you want Norton System Doctor to automatically start when Windows starts.

While the default settings are ideal for most users, Norton System Doctor is customizable. For example, you can do the following:

- Specify the conditions that Norton System Doctor monitors by adding and removing sensors.
- Select the critical conditions that you want Norton System Doctor to fix automatically.
- Run Norton System Doctor minimized or docked to preserve valuable desktop space.

See "Use online Help" on page 93.

For more information about Norton System Doctor capabilities and customization, see the online Help.

To set Norton System Doctor startup options

1 On the left side of the main window, click **Norton Utilities** > **Find and Fix Problems** > **Norton System Doctor**.

2 In the Norton System Doctor main window, click **View** > **Options**.

3 In the Norton System Doctor Options dialog box, on the Window Settings tab, in the Startup Options group, check or uncheck an option. Your options are:

Start Automatically with Windows	Norton System Doctor starts automatically the next time that Windows starts.
Start Minimized	The Norton System Doctor window is minimized when it starts.

4 Click **OK**.

Set Norton CleanSweep options

The default settings for Norton CleanSweep provide a safe and efficient way of removing unwanted files from your computer. Use the settings to optimize system performance or disable options that do not apply. From the Norton SystemWorks main window, you can access the following Norton CleanSweep options:

Norton CleanSweep options	Let you specify how installations and other files are monitored so that they can be easily removed later. You can also specify file names and locations for backup and log files.
Fast & Safe Cleanup options	Let you specify the types of unnecessary files that Fast & Safe Cleanup should delete, including Internet history, Internet cache, Recycle Bin, lost clusters, and Windows temporary files. You can also schedule cleanup of these files.

To set Norton CleanSweep options

1 On the Options menu, click **Norton CleanSweep**.

2 In the Norton CleanSweep Options dialog box, click a tab that contains the options that you want to change. The tabs and options are:

Safety Sweep	Fast Analysis ■ Indicate that Safety Sweep should scan to find all files that are related to an installed program. This helps to ensure that all of a program's related files are removed when you uninstall it. When Fast Analysis is turned off, the analysis takes longer but is more thorough. Safety Sweep ■ Enable and disable Safety Sweep. When Safety Sweep is enabled, only green items can be deleted by Fast & Safe Cleanup, and all items are backed up. Safety Sweep must be disabled before Cookie Cleanup can remove cookies that are marked yellow.
Smart Sweep/ Internet Sweep	Turn Smart Sweep/Internet Sweep On or Off ■ (Windows 98/Me only) Start or quit monitoring your computer with Smart Sweep and Internet Sweep. Load Smart Sweep/Internet Sweep on Startup ■ Indicate if Smart Sweep and Internet Sweep should start when Windows starts. Automatically Monitor Installs When Loaded ■ Indicate if Smart Sweep should always monitor installation activities when you install programs without asking you. Specify Program Names ■ (Windows 98/Me only) Indicate the names of installation programs that Smart Sweep should always monitor. View or Delete Smart Sweep/Internet Sweep Logs ■ View or clear the Smart Sweep/Internet Sweep activity text files.

Backup/Restore	Specify a default backup folder ■ Specify a folder where Norton CleanSweep keeps backups of uninstalled programs. The default is a backup folder inside of the Norton CleanSweep program folder. Specify confirmation in Uninstall Wizard ■ Indicate if you want Norton CleanSweep to ask you for confirmation before it uninstalls a program. Specify action in Restore Wizard ■ Indicate if, when restoring, you want to overwrite a file if it already exists. Specify backup reminder for older backups ■ Indicate if you want Norton CleanSweep to ask if you want to keep backups of uninstalled programs after 30 days.
View	View Master Log ■ View, clear, save, and print the Master Log. View folder usage ■ Display disk space that is used on available disk drives. Specify report file location ■ Specify the location for the log of Norton CleanSweep activities.

Use the Norton CleanSweep Master Log

The Master Log contains a record of all Norton CleanSweep activities in chronological order. You can view, clear, save, and print the Master Log.

To use the Norton CleanSweep Master Log

1. On the Options menu, click **Norton CleanSweep**.
2. In the Options dialog box, on the View tab, click **View Master Log**.
3. In the Master Log, select the action that you want to take. Your options are:

View the entire log	Drag the scroll bar down.
Clear the log	Click **Clear**.

Save the log in another location or with a different name	Click **Save.**
Print the log	Click **Print.**

4 When you are finished, click **Close**.

Set Fast & Safe Cleanup options

You set Fast & Safe Cleanup options after you start Fast & Safe Cleanup.

To set Fast & Safe Cleanup options

1 On the left side of the main window, click **Norton CleanSweep** > **CleanUp** > **Fast & Safe Cleanup**.

2 In the Fast & Safe Cleanup window, click **Settings**.

3 In the Fast & Safe Cleanup Settings dialog box, click a tab that contains the options that you want to change. The tabs and options are:

File Types	Internet Cache ■ Deletes all of the files in your Web browser's cache folder. If you use more than one browser, Fast & Safe Cleanup removes the files in each browser's cache folder. Internet History ■ Clears your browser's Internet history. The history contains links to all of the Web pages that you have visited recently. Empty Recycle Bin ■ Deletes all of the files in the Windows Recycle Bin. Temporary Files ■ Deletes all temporary files from your Windows\Temp folder. Temporary files are unnecessary files that other programs have created and not deleted. Lost Cluster Files ■ Deletes all lost cluster files. Cluster files are created by the Windows system utilities CheckDisk and ScanDisk.
Schedule	At system startup ■ Deletes all of the files in selected categories after Windows starts. Every xx days at xx ■ Deletes files in selected categories on a specific day and time.

4 Click **OK**.

Customize Norton AntiVirus

The default settings for Norton AntiVirus provide complete virus protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply.

Norton AntiVirus provides password protection for your option settings. You can enable, change, and reset a password so that unauthorized users cannot tamper with your settings.

All of the options are organized into three main categories. The options contained under each category are as follows.

Category	Options
System	Auto-Protect Manual Scan
Internet	Email Instant Messenger LiveUpdate
Other	Threat Categories Inoculation (Windows 98/98SE/Me) Miscellaneous

This section does not describe how to change the individual options, but gives a general description of what they do and how you can find them. For specific information about a particular option, check the online Help.

About System options

The System options control scanning and monitoring of your computer. You use System options to determine what gets scanned, what the scan is looking for, and what happens when a virus or virus-like activity is encountered.

With higher levels of protection, there can be a slight trade-off in computer performance. If you notice a difference in your computer's performance after installation, you may want to set protection to a lower level or disable those options that you do not need.

The System options that you can set are as follows.

Option	Description
Auto-Protect	Determine if Auto-Protect starts when you start your computer, what it looks for while monitoring your computer, and what to do when a virus is found. Auto-Protect options also include Bloodhound, Advanced, and Exclusions subcategories. ■ Bloodhound is the scanning technology that protects against unknown viruses. Use these options to set its level of sensitivity in Auto-Protect. ■ Advanced options determine the activities to be monitored when scanning for virus-like activities and when scanning floppy disks. ■ Exclusions specify the files that should not be scanned by file name extension or by specific file name. Be careful not to exclude the types of files that are more likely to be infected by viruses such as files with macros or executable files.
Manual Scan	Determine what gets scanned and what happens if a virus or threat is found during a scan that you request. Manual Scan options also include Bloodhound and Exclusions subcategories.

About Internet options

Internet options define what happens when your computer is connected to the Internet. You use Internet options to define how Norton AntiVirus should scan email and instant messenger attachments, enable Worm Blocking, and determine how updates should be applied with LiveUpdate.

The Internet options you can set are as follows.

Option	Description
Email	Enable email scanning and Worm Blocking, and define how Norton AntiVirus should behave while scanning email messages. Scanning incoming email messages protects your computer against viruses sent by others. Scanning outgoing email messages prevents you from inadvertently transmitting viruses or worms to others. You can choose to scan incoming or outgoing email messages, or both, and to display an icon or progress indicator while scanning. You can set options to automatically repair, quarantine, or delete infected email messages with or without interaction with you. Advanced options determine what to do when scanning email messages.
Instant Messenger	Determine what instant messengers to support, how to configure a new instant messenger, and what happens if a virus is found during an instant messenger session.
LiveUpdate	Enable Automatic LiveUpdate and define how updates should be applied. Automatic LiveUpdate checks for updated virus definitions automatically when you are connected to the Internet.

About Other options

Other options include Inoculation settings for Windows 98/98SE/Me and Miscellaneous settings. You can enable Inoculation, cause an alert if a system file changes, set a variety of miscellaneous options, and customize behavior for the Norton Protected Recycle Bin.

The Other options that you can set are as follows.

Option	Description
Threat Categories	Determine the threats that you want Norton AntiVirus to detect. Advanced options include how to respond when a threat is found and what to do when deleting threats. Exclusions options specify the files that should not be scanned by file name extension or by specific file name.
Inoculation	Enable Inoculation and, if a system file changes, choose to update the Inoculation snapshot or repair the file by restoring it to its original values. Inoculation options are available only on Windows 98/98SE/Me.
Miscellaneous	Back up file in Quarantine before attempting a repair. (This option is automatically set to On.) Enable Office Plug-in. If you upgrade to Microsoft Office 2000 or later after Norton AntiVirus is installed, you must enable this option to automatically scan Microsoft Office files. Alert me if my virus protection is out of date. Scan files at system startup (Windows 98/98SE only). Enable password protection for options.

Set Norton AntiVirus options

You change the settings for Norton AntiVirus options in the Options window.

If you set a password for Options, Norton AntiVirus asks you for the password before you can continue.

To change settings

1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.

2 In the Options window, in the left pane, select an option in the list.
Options with an arrow to the left have sub-options. As

you select an option, the corresponding settings for the selected option appear in the right pane.

3 Select any settings that you want to change.

4 Click **OK**.
These settings now take precedence over the preset options. The changes take effect immediately.

If you need to restore default Norton AntiVirus settings

You can change any or all of the options listed. If you have made a number of changes that have unwanted results, you can restore all options to the default settings.

! If you set a password for Options, Norton AntiVirus asks you for the password before you can view or adjust the settings.

To restore default settings on an Options page

❖ On the page for which you want to restore default settings, click **Page Defaults**.

To restore default settings for all options

❖ On any page in the Options window, click **Default All**.

Password protect Norton AntiVirus options

To protect your Norton AntiVirus options from being changed without your permission, you can choose to protect or remove protection from your option settings with a password. If you specify a password, you are asked to enter a password every time that you view the Options window, or temporarily enable or disable Auto-Protect.

If you forget your password, you can reset it from the Help button in the Norton AntiVirus main window. See the online Help for more information about resetting your password.

To specify or remove a password

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under Other, click **Miscellaneous**.
3. Check or uncheck **Enable password protection for options**.
4. In the password dialog box, type a password.
5. Click **OK**.

Set Wipe Info options

You can specify how Wipe Info handles files with *hidden*, read-only, and system attributes. You can also specify the type of wipe to use. The following wiping methods are available:

Fast Wipe	Overwrites the data that is being wiped with the hexadecimal value of your choice
Government Wipe	Combines several wiping and overwriting processes to conform to specifications in DoD (United States Department of Defense) document 5220-22-M, National Industrial Security Program Operating Manual, for the ultimate security level when eliminating data from digital media See "About the Government Wipe process" on page 248.

To change Wipe Info options in Windows 2000/XP

1 On the left side of the main window, click **Norton Utilities** > **System Maintenance**.

2 In the right pane, click **Wipe Info**.

3 In the Wipe Info window, on the View menu, click **Options**.

4 On the General tab, select the options for Read-only, System, and Hidden file types.

5 On the Wipe Type tab, select the type of wipe that you want to perform. Your options are:

- Fast Wipe
- Government Wipe

See "About hexadecimal values" on page 248.

6 In the Hex Value text box, type the hexadecimal values that Wipe Info should use when it overwrites the wiped files space.

7 In the Times to Perform This Wipe text box, type the number of times that Wipe Info should repeat this process.

8 Click **Apply**.

Set Norton Password Manager options

You can change the settings for the currently signed in profile in the Norton Password Manager Options dialog box. The following options are available:

Options	Enable or disable startup options. See "Set a profile's general options" on page 128.
Profile Name	Change a profile account name or region, or back up and restore profile data. See "Change profile information" on page 128.
Password	Change your profile password. See "Set up a Norton Password Manager profile" on page 156.
Identity	Change the name that is associated with this profile.
Addresses	Add, change, or remove a home, work, or other address. See "Change profile addresses" on page 130.
Credit Cards	Add, change, or remove a credit card. See "Change profile credit cards" on page 131.
Security Level	Change the security level for Norton Password Manager. See "Set Norton Password Manager options" on page 127.
Managed Passwords	View or remove the Windows programs and Web sites for which Norton Password Manager provides your password. See "View or delete managed passwords" on page 133.
Ignored Passwords	View or remove the Windows programs and Web sites for which Norton Password Manager does not provide your password. See "View or delete ignored passwords" on page 133.
Ignored Quick Fill Sites	View or remove Windows programs and Web sites.

Set a profile's general options

You can customize Norton Password Manager's startup settings, create profile backups, and restore profile data in the General Options dialog box.

To change Norton Password Manager general options

1. On the Options menu, click **Password Manager**.
2. Your options are:

Startup Options	■ Enable Norton Password Manager at startup: Norton Password Manager will respond if you sign in to a Web site or program. ■ Enable Web Browser support: Norton Password Manager will manage your passwords and fill in forms. ■ Enable Windows Program support: Norton Password Manager will sign in to Windows programs that require a password. ■ Enable Automatic LiveUpdate: LiveUpdate checks for and installs program updates without prompting you. LiveUpdate displays an alert when a program update has been downloaded.

Change profile information

Each Norton Password Manager profile must have a unique name. You can change the profile name and the country or region.

To change a profile name

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Current Profile**.
2. In the lower right of the window, click **Modify**.

3 On the left side of the Norton Password Manager Profile Options dialog box, make sure that Profile Name is selected.

4 If you are prompted for a password, type it.

5 Make changes to the Profile Name.

6 Click **OK**.

See "Back up or restore your profile information" on page 166.

You can also back up and restore profile data in this dialog box.

Change profile passwords

See "About strong passwords" on page 155.

You can change the password for a profile.

To change a profile password

1 On the left side of the main window, click **Password Manager** > **Status & Settings** > **Current Profile**.

2 In the lower right of the window, click **Modify**.

3 On the left side of the Norton Password Manager Profile Options dialog box, click **Password**.

4 In the Password text boxes, type your old password, type a new password, confirm the password by typing it again, then type a password hint.

5 Click **more info** for advice on creating a strong password.

6 Click **OK**.

Change profile identity

You can change the name that is associated with this profile. This name is used to fill in Web forms and programs.

To change a profile identity

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Current Profile**.
2. In the lower right of the window, click **Modify**.
3. On the left side of the Norton Password Manager Options dialog box, click **Identity**.
4. In the First Name, Middle Name, and Last Name text boxes, type the name that you want to use for this profile.
5. Click **OK**.

Change profile addresses

In Norton Password Manager you can add a home, work, and other address.

If you need to include additional addresses, consider creating a different profile.

To change a Norton Password Manager profile address

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Addresses**.
2. In the lower right of the window, click **Details**.
3. Select an address type, for example, Home, Work, or Other.
4. In the address information dialog box, type the street address, phone and fax numbers, and your email address.
5. To change another address in this profile, select it and change the information.
6. Click **OK**.

Change profile credit cards

You can change the credit card for a profile.

To change a Norton Password Manager profile credit card

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Credit Cards**.
2. In the lower right of the window, click **Details**.
3. Select the credit card that you want to change.
4. Change the available settings. Your options are:

Card Type	Select the type, for example, Visa, MasterCard, or American Express.
Card Description	Type a description that will help you identify this credit card.
Name on Card	Type the name as it appears on the credit card.
Card Number	Type the entire credit card number.
Expiration Date	Type the expiration date on the card.
Card Verification Number	Type the unique verification number for this card. This is usually located above the credit card number on the front of the card, or near the signature area on the back of the card.
Billing Address	Select the address to which the credit card statement is sent.

5. Click **OK**.

Change profile security level

You can change the frequency that Norton Password Manager requires you to sign in with your profile password.

To change the profile's security level

1. On the left side of the main window, click **Password Manager** > **Security Level**.
2. Change the available settings. Your options are:

High	You must type your profile password every time that you are prompted to enter any private information. This option provides the highest level of security.
Medium	After you type your profile password, Norton Password Manager requests it again after the specified period of keyboard and mouse inactivity. This option protects you but does not cause you to type your profile password as frequently as the High option.
Low	You must type your profile password only once, when you start Norton Password Manager. This option is the least secure, in cases where your unattended computer might be used by someone else who could use your private information indiscriminately.

View or delete managed passwords

When Norton Password Manager remembers a Web site password, the Web site is added to the managed passwords list. You can view or delete the Web sites on this list.

If you delete a site from the managed passwords list and then visit the site again, Norton Password Manager asks you if you want to remember the password again.

To view or delete a managed program or Web site

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Passwords**.
2. On the left side of the Norton Password Manager Options dialog box, ensure that Managed Passwords is selected.
3. To remove a program or site from the list, select it, then click **Remove**.
4. Click **OK**.

View or delete ignored passwords

If you have specified that Norton Password Manager should not sign in to a program or Web site, it is added to the Ignored Passwords list. If you want Norton Password Manager to stop ignoring the program or site, remove it from the list.

To stop ignoring a program or Web site's password

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Passwords**.
2. In the lower right of the window, click **Details**.
3. On the left side of the Norton Password Manager Options dialog box, click **Ignored Passwords**.
4. To remove a program or site from the list, select it, then click **Remove**.
5. Click **OK**.

View or delete ignored Quick Fill sites

If you want Norton Password Manager to fill in your profile information, remove the Web site or Windows program from the Ignored Quick Fill Sites list.

To view or delete an ignored Quick Fill site

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Passwords**.
2. In the lower right of the window, click **Details**.
3. On the left side of the Norton Password Manager Options dialog box, click **Ignored Quick Fill Sites**.
4. To remove a program or site from the list, select it, then click **Remove**.
5. Click **OK**.

Improving Web browsing and connectivity

6

There are two programs that make your Internet activities more efficient and reliable. Web Cleanup lets you quickly and safely delete the files and data that accumulate after you browse the Internet. Connection Keep Alive lets you maintain your *dial-up* Internet connection even when you're not actively using the connection.

About Web Cleanup

Web Cleanup locates and deletes temporary files and data items that collect on your computer after you browse the Internet with Internet Explorer. These items accumulate in your computer's Internet history and temporary *cache* file storage areas. Most of these temporary files have little value, occupy disk space, and slow down your computer's performance.

Web Cleanup works only with Internet Explorer and its associated files.

Web Cleanup lets you view the contents of files before you delete them. You can add *domain names*, or URLs, to a list so that Web Cleanup doesn't select them for deletion again.

Certain types of files, such as *cookies*, store personal data. You might want to keep these files to save the effort of repeatedly logging onto a frequently used, secure site. However, this personal data could be the target of hackers or other malevolent programmers.

With Web Cleanup, you can:

- Automatically delete all unnecessary Web files and related data items with Quick Clean.
- View individual files and other Internet items to save or delete with Advanced Cleanup.

Delete unnecessary Web files

Quick Clean scans for files that are typically left behind after Internet browsing. These include Internet history and *cache* files, and *cookies*. At the completion of the scan, you have the option to delete all of the files that were found during the scan.

See "View Web Cleanup files" on page 136.

If you want to see more information about the files before they are deleted, you can select them individually using Advanced Cleanup.

To delete unnecessary Web files

1. On the left side of the main window, click **Web Tools** > **Web Cleanup**.
2. Click **Begin Quick Clean**.
   Quick Clean scans your computer and displays a summary of files and other Internet items that can be deleted.
3. Click **Cleanup Now!** to delete all of the summarized items automatically.
4. Click **Finish**.

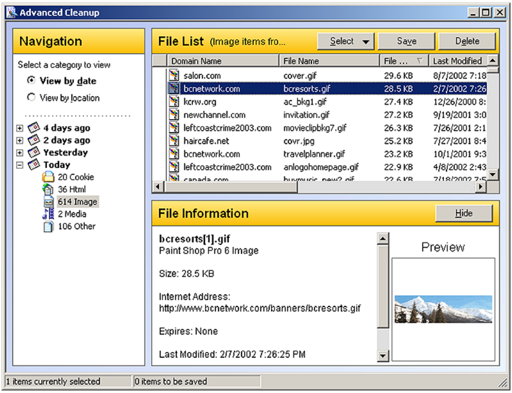
View Web Cleanup files

Web Cleanup lets you view detailed information about all of the files that are selected for deletion. You can view a selected file's creation date, type, contents, and other information. Viewing information helps you determine if a file should be deleted or saved.

To view Web Cleanup files

1 On the left side of the main window, click **Web Tools** > **Web Cleanup**.

2 Click **Advanced Cleanup**.



Domain Name	File Name	File ...	Last Modified
salon.com	cover.gif	29.6 KB	8/7/2002 7:18
bcnetwork.com	bcresorts.gif	28.5 KB	2/7/2002 7:26
kcrw.org	ac_bkg1.gif	27.4 KB	12/26/2000 8:
newchannel.com	invitation.gif	27.2 KB	9/19/2001 3:0
leftcoastcrime2003.com	movieclipbkg7.gif	26.3 KB	7/26/2001 2:1
haircafe.net	covr.jpg	25.2 KB	7/27/2001 8:4
bcnetwork.com	travelplanner.gif	23.2 KB	10/1/2001 9:3
leftcoastcrime2003.com	anlogohomepage.gif	22.9 KB	4/8/2002 2:43
canada.com	buymusic_new2.gif	22.6 KB	7/18/2002 7:5

bcresorts[1].gif
Paint Shop Pro 6 Image

Size: 28.5 KB

Internet Address:
http://www.bcnetwork.com/banners/bcresorts.gif

Expires: None

Last Modified: 2/7/2002 7:26:25 PM

3 In the Navigation pane, select how to display the grouped categories. Your options are:

View by date	File categories are listed chronologically with the most recently viewed Web site files listed first.
View by location	File categories are listed alphanumerically by the associated Web site domain name, IP address, or other identifying name.

4 In the Navigation pane, click the plus sign next to a Web site or category (History, HTML, image, cookie) to display its contents.

5 Click an item.

6 Under Domain Name, click a file category to display individual files in the File List.

7 To close the File Information pane and view more items in the File List, click **Hide**.

8 To sort the File List, click a column heading.
Expand the window or use the horizontal scroll bar to see more columns. The columns include the following information:

Domain Name	Web site name or URL
File Name	File name on the disk
File Size	The size in bytes on your hard disk
Last Modified	The date when the file was last changed on the hard disk
Expires	If the file is a cookie, the date when it expires
Last Sync	If the file is a synchronized file, the date when the item was last synchronized with another device (such as a handheld device)
Last Accessed	The date when the domain name was last accessed from your computer

9 In the File List, select an item to display more information in the File Information pane.
If you closed the File Information pane, click **Show**.

10 In the File List, select one or more items using one of the commands on the Select menu.

11 Identify what to do with the selected items. Your options are:

Save	Add the item to the Web Cleanup tab in the Web Tools Options dialog box. Domains in this list will not be deleted by Quick Clean.
Delete	Remove the selected file from the Viewer List, but do not delete the file. It will show up in the scan next time, unless you add it to the list of excluded Web sites in the Web Cleanup Options list.

If you saved a domain name, in the alert message, click **OK**.

12 When you are finished, close the View Files window.

Exclude domains from Web Cleanup activity

You can list Web *domain names* whose files should be excluded from Web Cleanup activity. Along with the domain names, you can specify which categories of files, *cookies*, *cache*, or history, should be protected.

It might help to have your Internet browser open to a Web site’s home page as you are typing, so that you can refer to the correct spelling of the domain name in your browser’s address line.

You can type the domain names directly in the Web Cleanup dialog box. You can also select them in the Advanced Cleanup file list.

To exclude domain names in the Web Cleanup list

1 On the Options menu, click **Web Tools**.

2 In the Web Cleanup dialog box, click **Insert**.

3 Type the domain name that you want to exclude from deletion, then press **Enter**.
For example, type www.symantec.com to add the Symantec Web site to the list.

4 For the domain, select the types of files that you want to exclude from Web Cleanup activity. Your options are:

Cookies	Any cookies that are associated with the domain
Cache	Any cache files that are associated with the domain
History	Any history files of Internet activity that include the domain name

5 Click **Apply**.

6 Repeat steps 2 to 5 until you have added all of the domain names that you want to exclude from Web Cleanup activity.

7 Click **OK**.

To exclude domain names in the Advanced Cleanup File List

1 On the left side of the main window, click **Web Tools** > **Web Cleanup**.

2 In the Web Cleanup main window, click **Advanced Cleanup**.

3 In the Advanced Cleanup window, in the File List, select one or more items using one of the commands on the Select menu.

4 Click **Save**.
The domain name is added to the list of domains in the Web Cleanup dialog box.
All file categories for the domain, including cookies, cache, and history, are checked.

5 Repeat steps 3 and 4 until you have selected all of the domain names that you want to exclude from Web Cleanup activity.

About Connection Keep Alive

Connection Keep Alive prevents your *dial-up* Internet connection from disconnecting when you want to stay connected, but are not browsing the Internet, using email, or performing another Internet activity. Connection Keep Alive sends a small signal to a Web site. This prevents your Internet service provider (*ISP*) from canceling the connection.

Some ISPs might not allow this activity. Read your ISP's User Agreement before you enable Connection Keep Alive.

Enable or disable Connection Keep Alive

You can enable Connection Keep Alive whenever you need it. You can also specify how long you want to stay connected before Connection Keep Alive quits.

You can enable or disable Connection Keep Alive from the main window or from the Windows system tray.

To enable or disable Connection Keep Alive from the main window

1. On the left side of the main window, click **Web Tools** > **Connection Keep Alive**.
   The Connection Keep Alive status indicates whether it is On or Off.
2. Select one of the following:
   - Enable
   - Disable

To enable or disable Connection Keep Alive from the system tray

1. In the Windows system tray, right-click the Connection Keep Alive icon.
2. Select one of the following:
   - Enable Connection Keep Alive
   - Disable Connection Keep Alive

View Connection Keep Alive status

After you have used Connection Keep Alive for the first time, you can view whether it is enabled or disabled in the following ways:

- When it is disabled, the Connection Keep Alive Windows system tray icon has a small X.
- If Norton Tray Manager is in your computer's Windows system tray, hold the mouse cursor over the Norton Tray Manager icon until the Connection Keep Alive icon pops up. A tooltip displays its status.
- In the Connection Keep Alive main window, the Connection Keep Alive panel indicates its status as ON (enabled) or OFF (disabled).

Set Connection Keep Alive options

You can specify if Connection Keep Alive should start when Windows starts, the level of activity it uses, the Web sites to which it sends signals, and when to stop sending signals. You can access Connection Keep Alive options from the Norton SystemWorks main window or from the Windows system tray.

To set Connection Keep Alive options from the main window

1. On the Options menu, click **Web Tools**.
2. On the Connection Keep Alive tab, change the settings. Your options are:

Automatically start with Windows	Connection Keep Alive is enabled when Windows starts.
Display splash screen on startup	Connection Keep Alive displays a splash screen when Windows starts.

Keep Alive Level Low/High	The frequency with which Connection Keep Alive sends signals to (pings) its network. For UDP and ICMP network communications protocols, the Low or High settings can be used. For the HTTP communications protocol, only the High setting is used.
Network traffic destination My Favorites My Homepage <ping.symantec.com>	When it simulates network traffic, Connection Keep Alive pings the Web sites in My Favorites, My Homepage, the Symantec Web site, or ping.symantec.com. You can replace ping.symantec.com with your own choice. ⚠ If the Keep Alive Level is set to High, and you specify a different Web site to ping, be sure to include the HTTP prefix, for example http://www.myownurl.com
Simulate network activity every XX minute(s)	Connection Keep Alive sends a signal every 1, 2, 3, or more minutes, up to 15. The default is 1 minute.

Disable when inactive for more than XX minute(s)	If there is no mouse or keyboard activity, Connection Keep Alive disables itself after the indicated period.
Display timeout warning message	Connection Keep Alive displays a warning message before it disables itself after the scheduled number of minutes. The message remains for a countdown of 60 seconds. If you respond to the message, Connection Keep Alive remains active.

3 When you are finished, click **OK**.

To set Connection Keep Alive options from the Windows system tray

1 In the Windows system tray, right-click the Connection Keep Alive icon, then click **Connection Keep Alive Options**.

2 In the Connection Keep Alive Options dialog box, change the settings.

3 Click **OK**.

Reverting your hard disk

Norton GoBack protects you from data loss by integrating into your computer's operating system, recording all changes to your hard disk.

With Norton GoBack, you can:

- Revert your hard disk to a specific date and time
- Provide Norton GoBack protection to programs that require a special boot disk to get it started

⚠ To be able to restore your computer to a past date and time, Norton GoBack must already be installed and enabled on your hard disk.

About Norton GoBack

Norton GoBack keeps track of every event that takes place on your hard disk and then allows you to revert - or "go back" - to an earlier time if any errors or software problems occur. With Norton GoBack, you can easily back out of trouble, regardless of whether the problem was caused by you or by the software on your computer.

⚠ Norton GoBack is not a replacement for the need to backup your files. Norton GoBack does not prevent data loss if your hardware actually breaks or if the data you desire was altered long ago. This is why a traditional backup routine is still important to maintain.

About reverting a disk

The reason you would use Norton GoBack to revert your hard disk to a date and time in the past is because you don’t know exactly which files to restore, or you don’t know exactly what went wrong. All you know is that a problem has occurred.

Perhaps it was new software that you attempted to install and the result was that your computer is not working correctly since the installation. Or, you tried adding a new device driver and it caused your computer to slow down or not work properly.

Another example of when to use Norton GoBack would be if you printed an email or document, then erased or deleted what you printed, only to find that the printed copy is lost or unreadable. In this case, you would want to revert to the date and time before you erased the data.

About Norton GoBack safe points

Norton GoBack continually monitors all hard disk activity, and when it determines that nothing has been written to the hard disk for several seconds, it makes a note - called a safe point - in its log.

When you want to revert your hard disk to a past date and time, Norton GoBack lets you select from a set of safe points because you generally wouldn’t want to choose a time when you were in the middle of saving a file.

If you perform several file activities in rapid succession, such as writing a file and then immediately deleting it, Norton GoBack may not have written a safe point in the log. If this happens, you may not be able to select a time between these activities. To avoid this situation, pause between disk activities to allow the hard disk time to catch up.

Under certain circumstances, Norton GoBack safe points may be erased. This can happen when you optimize your hard disk with Speed Disk, download large files from the Internet, scan your computer with Norton AntiVirus, or wipe free space on your hard disk with Wipe Info. If the safe points are erased, Norton GoBack creates new ones in a short time.

Start Norton GoBack

You can start Norton GoBack from the Start menu, from the Windows system tray, from a shortcut on your desktop, or during your computer's startup process.

To access Norton GoBack from the Start menu

- ❖ Do one of the following:
  - On the Windows taskbar, click **Start** > **Programs** > **Norton GoBack**.
  - On the Windows XP taskbar, click **Start** > **All Programs** > **Norton GoBack**.

To access Norton GoBack from the Windows system tray

- ❖ In the Windows system tray, click the Norton GoBack icon.

To access Norton GoBack from the desktop

- ❖ On the Windows desktop, double-click the Norton GoBack icon.

To access Norton GoBack during startup

1. Restart your computer.
2. As soon as the Norton GoBack Boot Screen appears, press the spacebar.

Revert your hard disk

Norton GoBack automatically runs whenever you start your computer. If a problem occurs, you can select from a series of safe points so that your hard disk reverts to a previous date and time before the problem occurred.

To revert your hard disk

See "Start Norton GoBack" on page 147.

1. In the Norton GoBack main window, click **Revert your hard drive**.
2. In the list of Event Types, select a System Safe Point, or Start of System Boot with a date and time just prior to when the problem occurred.
3. After you have selected an event, click **Revert Now**.
   A message informs you that in order to revert your hard disk, your computer must restart.
4. Click **OK**.
   A Norton GoBack progress bar appears. After your computer restarts, your hard disk will be reverted to the date and time selected.

Revert your hard disk from the Norton GoBack boot menu

If your computer fails to start normally and you are unable to run Windows, you can use the Norton GoBack boot menu, which starts before Windows, to revert your hard disk back to a date and time when Windows was operating normally.

If you choose to revert with the boot menu, it is best to use the most recent safe point listed. If the revert is not successful, revert again using a different date and time. Generally, the first one or two attempts will succeed in letting your computer's operating system start again.

To revert your hard disk from the boot menu

1. Restart your computer using the power switch, the reset button, or by pressing **Ctrl**+**Alt**+**Delete**.
2. As soon as you see the Norton GoBack Boot screen appear, press the spacebar.
3. Click **Revert Drive**.
4. In the Safe Points list, select a date and time.
   If you need to see more safe points, click **More Times**.
5. Click **Revert**.
   A message informs you that in order to revert your hard disk, your computer must restart.

6. Click **Yes**.
   A Norton GoBack progress bar appears.
7. Click **OK**.
   After your computer restarts, your hard disk will be reverted to the date and time selected.

Boot from a floppy disk with Norton GoBack protection

For programs requiring a floppy disk to get started, you can use Norton GoBack to ensure that, if needed, you can revert back to a date or time before you ran the program.

To boot from a floppy disk

1. Restart your computer.
2. When the Norton GoBack Boot screen appears, press the spacebar.
3. Insert the program's floppy disk into drive A.
4. On the Norton GoBack boot menu, click **Boot from Floppy**.
   Your computer will boot into the program.

Clear your computer's history

Norton GoBack lets you clear your computer's history to prevent anyone from seeing information that has been changed or deleted.

When you clear Norton GoBack history, you also take away your ability to revert to the times that you have cleared. Norton GoBack cannot restore a history that you have cleared.

To clear Norton GoBack history

1. In the Norton GoBack main window, click **Options**.
2. Select the drive you wish to clear.
3. Click **Clear Norton GoBack History**.
   A message informs you that clearing the history is a permanent action that cannot be undone.
4. To continue clearing the history, click **Yes**.

Disable or enable Norton GoBack

When you disable Norton GoBack, all history information is cleared and you will be unable to revert your hard disk until Norton GoBack is enabled again.

You can disable Norton GoBack from the main window or from the boot menu.

⚠ Norton GoBack will not track any information while it is disabled.

See "Use online Help" on page 93.

For more information, see the online Help.

Disabling Norton GoBack requires that you restart your computer.

See "Start Norton GoBack" on page 147.

To disable Norton GoBack from the main window

1. In the Norton GoBack main window, click **Options**.
2. Click **Disable Norton GoBack**.
   A message informs you that disabling Norton GoBack will clear the history and prevent any reverting.
3. Click **OK**.
   Your computer will automatically restart and Norton GoBack will be disabled.

To disable Norton GoBack from the boot menu

1. Restart your computer.
2. When the Norton GoBack Boot Screen appears, press the SPACEBAR.
3. On the Norton GoBack boot menu, click **Disable**.
   A message will appear letting you know that disabling Norton GoBack will clear the history and you will no longer be able to recover data from the past.
4. Click **Yes**.
5. Click **Continue**.
   Your computer will automatically restart and Norton GoBack will be disabled.

To enable Norton GoBack

See "Start Norton GoBack" on page 147.

1 Start Norton GoBack.
A message will appear reminding you that Norton GoBack is currently disabled.

2 Click **Yes** to enable Norton GoBack.
Your computer will automatically restart and Norton GoBack will be enabled.

Hide/show the Norton GoBack Windows system tray icon

When Norton GoBack is installed, its icon automatically appears in the Windows system tray for easy access when you need to restore your hard disk.

To hide the Norton GoBack icon in the Windows system tray

1 In the Norton GoBack main window, click **Options**.

2 Uncheck **Icon in System Tray**.
If the box is checked, the icon appears in the Windows system tray. If the box is unchecked, the icon is hidden.

Maintaining password security

8

Norton Password Manager protects your Windows program and Internet logon information, and stores address and credit card information for e-commerce transactions. Norton Password Manager automatically recognizes programs and Web sites that require you to log on, and, with your consent, provides the logon information automatically. The information you store in Norton Password Manager is encrypted.

Norton Password Manager also helps you to create passwords that are hard to guess. This increased security makes your computing activity more secure.

About profiles and passwords

See "Set up a Norton Password Manager profile" on page 156.

The profile password is the key to using Norton Password Manager. It is very important that you choose a password that you can remember, but that is strong enough so that someone else can't guess it and gain access to your private information.

To set up a Norton Password Manager profile, you need a profile name, your country or region, and an optional profile password. The other information that is requested by the profile wizard, including name, addresses, and credit card information, is optional. The more information that is included in a profile, the less information you have to type when you are shopping online, or signing in to a program or Web site.

About profiles

The Norton Password Manager profile contains two types of information:

- The information that you add when you set up the profile, including a profile name, a profile password, your name, address, and credit card information. You can add or change the address and credit card information after the profile is created.
- The logon IDs and passwords that Norton Password Manager collects from Web sites and Windows programs. This list is associated with a specific profile. Once Norton Password Manager has recorded this information, it can sign in for you automatically, or provide more limited information if you prefer to sign in manually. You can delete Web sites and Windows programs from this list.

About strong passwords

A strong password is your best defense against identity theft. That is why it is important for you to create the strongest possible profile password. When you create a profile password, Norton Password Manager assists you.

If the password that you type is less than seven characters, Norton Password Manager displays a message that prompts you to type more characters.

A strong password has the following characteristics:

- At least seven characters
- At least one capital letter
- At least one lowercase letter
- At least one numeral (0 through 9)
- At least one symbol (for example, * ^ & $ %)

Although you can create a profile password with as few as seven characters, a longer password is more secure.

Set up a Norton Password Manager profile

To use Norton Password Manager you must create at least one profile. The only information that is required in a profile is a unique profile name and country or region. You can create multiple profiles, but you must set up each profile with this same setup process.

To make a profile useful, you should add as much information as possible to it. The information is safely stored on your computer in an encrypted format.

The setup process includes creating a strong profile password, and then adding other private information. Later, when you are browsing the Web or running Windows programs, you can add logon information for Web sites and programs that require you to log on. You must create a profile before you can begin using Norton Password Manager. You can add more information to a profile at any time.

To set up a Norton Password Manager profile

1. Do one of the following:
   - In the Windows system tray, right-click the Norton Password Manager icon, then click **Create New User Profile**.
   - On the left side of the main window, click **Password Manager** > **Status & Settings**, then click **Create New Profile**.
     If you are signed in, click **Current Profile**, then click **New Profile**.
2. In the Profile Name window, type a unique name for the profile, select a country or region, then click **Next**.

   If you have already created a profile and backed it up, you can restore its data to the new profile.

See “Back up or restore your profile information” on page 166.

3 In the Password window, type a password, confirm the password by typing it again, then type a password hint. The hint should help you remember your password.

See "Change profile passwords" on page 129.

You can change a profile name or password later.

4 Click **Next**.

See "Change profile identity" on page 130.

5 In the Identity window, type the name that you want to use for this profile, then click **Next**.
This name will be used to fill in Web and program forms.

See "Change profile addresses" on page 130.

6 In the Addresses section, type a home, work, or other address, then click **Next**.
Each profile can have up to three addresses. You can add information for a home, work, and other address. Each address can include a street address, phone and fax numbers, and an email address.
If you don't want to add addresses to the profile now, you can add them later.

7 Click **Next** to skip ahead.

8 In the Credit Cards section, add credit card information, then click **Next**. Your options are:

Card Type	Select the type, for example, Visa, MasterCard, Discover, American Express, or Other.
Card Description	Type a description that will help you identify this credit card.
Name on Card	Type the name as it appears on the credit card.
Card Number	Type the entire credit card number.
Expiration Date	Type the expiration date on the card.

Card Verification Number	Type the unique verification number for this card. This is usually located above the credit card number on the front of the card, or near the signature area on the back of the card.
Billing Address	Select the Home, Work, or Other address to which the credit card statement is sent.

9 To add another card, click **Add Another Card**.

If you don't want to add credit cards to the profile now, you can add them later.

See "Change profile credit cards" on page 131.

10 In the Security Level window, select a security level, then click **Next**. Your options are:

High	You must type your profile password every time that you want to change any profile information. This option provides the highest level of security.
Medium	After you type your profile password, Norton Password Manager requests it again after the specified period of keyboard and mouse inactivity. This option protects you but does not cause you to type your profile password as frequently as the High option.
Low	You must type your profile password only once, when you start Norton Password Manager. This option is the least secure, in cases where your unattended computer might be used by someone else who could use your private information indiscriminately.

11 If you want to start using your profile right away, in the Setup Complete window, ensure that **Sign in to new profile now** is checked.
If you have signed into a profile, an alert box over the Windows system tray briefly displays the profile name.

12 Click **Finished**.

Access Norton Password Manager

You can start Norton Password Manager from the Windows Start menu, from a shortcut on the Windows desktop, and from an icon in the Windows system tray.

You can also close Norton Password Manager from the Windows system tray icon.

Start Norton Password Manager

From the Norton Password Manager main window you can use personal profiles, set options, run LiveUpdate, and perform other activities.

When Norton Password Manager is installed, its icon appears in the Windows system tray. You can access your profiles from here.

To start Norton Password Manager from the Windows system tray

1. In the Windows system tray, do one of the following:
   - Right-click the Norton Password Manager icon, then click **Open Norton Password Manager**.
   - Right-click the Norton Password Manager icon, then click **Sign In User Profile**.
2. In response to the confirmation message, click **Yes**.

To start Norton Password Manager from the Start menu or desktop

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** **> Norton SystemWorks** > **Norton Password Manager** > **Norton Password Manager**.
   - On the Windows XP taskbar, click **Start** > **All Programs** > **Norton SystemWorks** > **Norton Password Manager** > **Norton Password Manager**.

2 In the Norton Password Manager main window, do one of the following:

- If you have not yet created a profile, click **Create Profile**.
- If you have already created a profile, click **Sign In**, select a profile, then type your password.

See "Set up a Norton Password Manager profile" on page 156.

You must be signed in to a profile before you can view the status or options.

View a profile's status and settings

The Status & Settings window displays the status for the current profile.

To view a profile's status and settings

1 On the left side of the main window, click **Password Manager** > **Status & Settings**.

2 Select a feature to view its status. Your options are:

Current profile	The profile with which you signed into Norton Password Manager.
Passwords	The number of passwords that Norton Password Manager has for this profile. You can view details for this item.
Addresses	The number of addresses in the current profile. You can view details for this item.
Credit Cards	The number of credit cards in the current profile. You can view details for this item.
Security Level	The security setting in the profile. You can change this setting in the options or in the Security Level window.
Web Browser	Whether Norton Password Manager is monitoring Web sites. You can turn this setting on or off.
Windows Programs	Whether Norton Password Manager is monitoring Windows programs.

Close Norton Password Manager

Norton Password Manager normally starts with Windows. You can close the program in the Windows system tray.

To close Norton Password Manager

1. In the Windows system tray, right-click the Norton Password Manager icon, then click **Exit**.
2. In response to the confirmation message, click **OK**.
   To use Norton Password Manager again, you must start it from the Start menu.

Fill in forms with Norton Password Manager

You can use Norton Password Manager to automatically fill in Web forms and Windows programs with your private information. You can also use Norton Password Manager to select the data that you want to fill in manually. You can update and change your private information, including your addresses, telephone numbers, credit card information, and master password.

Because Norton Password Manager is available in the Windows system tray, it is available any time you want to add private information to an Internet form or Windows program.

About Internet forms

Norton Password Manager is designed to recognize most popular online forms.

Standard form fields include the following:

- First, middle, and last name
- Two address lines, for the street and suite number
- Phone number
- Email address
- Credit cards including Visa, MasterCard, American Express, Discover, and Diners Club

See "Fill forms manually" on page 164.

If a Web site form includes nonstandard information, Norton Password Manager cannot transfer the form data automatically with Quick Fill, but you can transfer it manually using Form Assistant.

Fill or ignore forms automatically

With your confirmation, Norton Password Manager automatically fills online transaction or shopping information, and inserts user names and passwords on password-protected Web pages and Windows programs.

See "Fill forms manually" on page 164.

Depending on the security level setting and the length of time that has elapsed since Norton Password Manager was used, you might need to type your profile password.

To fill or ignore Web forms automatically

1 In your browser, go to a Web site that requires you to type a personal ID or other personal data.

2 When Norton Password Manager asks if you want it to fill the form automatically, click **Fill Form**.
If this is the first time that Norton Password Manager has seen the site, it offers to remember your ID and password if you enter them.

3 Do one of the following:
- To add the information to the database, check **Yes**.
- To ignore the form this time, check **No**.
- To ignore the form permanently, check **Disable Quick Fill**, then click **No**.

See "Fill forms manually" on page 164.

If Norton Password Manager does not recognize the form, use Form Assistant to drag your private information into the Web site's text boxes.

To fill a Windows program automatically

See "Fill forms manually" on page 164.

1 Start the program where your private information is required.
Norton Password Manager should recognize the empty form. If it does not recognize the form, you can use Form Assistant.

2 When Norton Password Manager asks if you want it to fill the form automatically, click **Fill Form**.
The information in Norton Password Manager appears in the form.

3 If more information needs to be added manually, click **Go to Form Assistant**.

Fill forms manually

If a Web site or Windows program has a form that Norton Password Manager can't fill automatically, Norton Password Manager can assist you in filling the form so that you don't have to type the information again. Form Assistant displays the address and credit card information from your profile so you can select the profile information that you need.

Using Form Assistant you can select and drag the text, such as a credit card number, to the corresponding text box in your Internet browser or Windows program.

To fill a form manually

1. In your Web browser, go to the Web site where your private information is required.
   The Form Assistant dialog box might appear automatically. If the Quick Fill dialog box appears, you can change to the Form Assistant.
2. Click **Go to Form Assistant**.
   You can also start Form Assistant by right-clicking the Norton Password Manager icon in the Windows system tray.
3. Click in the text box that contains the text that you need, for example, your name.
4. Drag the pointer to the destination text box in the browser or program, then release the mouse button.
   The text should appear in the destination Internet or program box.
5. If you need to change the information that appears in Form Assistant, click **Click here to edit profile options**.

Manage your profile information

Norton Password Manager includes a utility that backs up profile information to an external file. You can use this file as a safety backup, and to transfer your information to Norton Password Manager on a different computer.

Norton Password Manager encrypts all profile data files. The data that you back up cannot be read or decrypted by other programs.

Back up or restore your profile information

Norton Password Manager maintains your private profile data in a database. You can back up the profile by exporting the data to an external, encrypted file. You can also use this export/import feature to migrate your profile information to a different profile, or to another licensed installation of Norton Password Manager.

To back up the profile database

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Current Profile**.
2. In the lower right of the window, click **Modify**.
3. On the left side of the Norton Password Manager Options dialog box, ensure that Profile Name is selected.
4. In the Profile Name dialog box, click **Backup Data**.
5. Type a file name, select the location for the backed-up file, then click **Save**.
6. Type a password that will be required to restore the backup.
7. Click **OK**.

ⓘ If you do not want to overwrite the data in the current profile, you can add a new, empty profile, sign into it, and import the backup file to fill in the new profile data.

To restore the profile database

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Current Profile**.
2. In the lower right of the window, click **Modify**.
3. On the left side of the Norton Password Manager Options dialog box, ensure that Profile Name is selected.
4. In the Profile Name dialog box, click **Restore Data**.
5. Click **Yes** to the warning that all data in the profile will be replaced.
6. Locate the backed-up file.
7. Click **Open**.
8. Type the password that was assigned to the backup, then click **OK**.

View or delete managed sites

Norton Password Manager keeps a list of all the Web sites and Windows programs for which you have recorded passwords.

If you do not want Norton Password Manager to automatically fill in private information on a managed site, you can delete it from this list.

To stop ignoring a program or Web site

1. On the left side of the main window, click **Password Manager** > **Status & Settings** > **Current Profile**.
2. In the lower right of the window, click **Modify**.
3. On the left side of the Norton Password Manager Options dialog box, click **Ignored Passwords**.
4. To remove a program or site from the list, select it, then click **Remove**.
5. Click **OK**.

Create multiple profiles

You can create separate accounts in Norton Password Manager that have different master passwords. If you have created multiple accounts, you will be prompted to select the account that you want to use.

To create another profile

1. Do one of the following:
   - On the left side of the main window, click **Password Manager** > **Status & Settings**, then click **Create New Profile**.
     If you are signed in, click **Current Profile**, then click **New Profile**.
   - On the left side of the main window, click **Password Manager** > **New Profile**.

See "Set up a Norton Password Manager profile" on page 156.

2. Follow the setup wizard instructions to add a profile ID, password, name, address, and other private information.

The completed profile is added to the Norton Password Manager profile list.

Change to a different profile

See "Create multiple profiles" on page 167.

If you have created more than one Norton Password Manager profile, you can select which one to use.

To change to a different profile

1 Do one of the following:
   - In the Windows system tray, right click the Norton Password Manager icon.
   - On the left side of the main window, click **Password Manager** > **Status & Settings** > **Current Profile**.

2 Click **Switch Profiles**.

3 In the Norton Password Manager Sign In dialog box, select another profile.

4 Type the password that is associated with the selected profile.

5 Click **Sign In**.

About the credit card verification number

Credit card companies include credit card verification numbers for extra security. Some companies require that you supply this number along with your credit card number.

The credit card ID number is usually located either above and to the right of the credit card number, or on the back of the card in the signature area. It is usually either four or seven digits long.

Keeping current with LiveUpdate

9

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

Your normal Internet access fees apply when you use LiveUpdate.

If your computer uses Windows 2000/XP, you must have Administrator *access privileges* to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files that are available from Symantec that keep your Symantec products up-to-date with the latest anti-threat technology. The protection updates you receive depend on which product you are using.

Norton AntiVirus, Norton AntiVirus Professional, Norton SystemWorks, Norton SystemWorks Professional, Symantec AntiVirus for Handhelds – Annual Service Edition	Users of Norton AntiVirus, Norton SystemWorks, and Symantec AntiVirus for Handhelds – Annual Service Edition products receive virus protection updates, which provide access to the latest virus signatures and other technology from Symantec.
Norton Internet Security, Norton Internet Security Professional	In addition to the virus protection updates, users of Norton Internet Security products also receive protection updates for Web filtering, intrusion detection, and Norton AntiSpam. The Web filtering protection updates provide the latest lists of Web site addresses and Web site categories that are used to identify inappropriate Web content. The intrusion detection updates provide the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access attempts to your computer. Norton AntiSpam updates provide the latest spam definitions and updated lists of spam email characteristics. These lists are used to identify unsolicited email.
Norton Personal Firewall	Users of Norton Personal Firewall receive intrusion detection updates for the latest predefined firewall rules and updated lists of applications that access the Internet.
Norton AntiSpam	Users of Norton AntiSpam receive the latest spam definitions and updated lists of spam email characteristics.

Obtain updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.

If your *Internet service provider* does not automatically connect you to the Internet, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. At the top of the main window, click **LiveUpdate**.
2. In the LiveUpdate window, click **Next** to locate updates.
3. If updates are available, click **Next** to download and install them.
4. When the installation is complete, click **Finish**.

Some program updates may require that you restart your computer after you install them.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Set LiveUpdate to Interactive or Express mode

LiveUpdate runs in either Interactive or Express mode. In Interactive mode (the default), LiveUpdate *downloads* a list of updates that are available for your Symantec products that are supported by LiveUpdate technology. You can then choose which updates you want to install. In Express mode, LiveUpdate automatically installs all available updates for your Symantec products.

To set LiveUpdate to Interactive or Express mode

1 At the top of the main window, click **LiveUpdate**.

2 In the LiveUpdate welcome screen, click **Configure**.

3 In the LiveUpdate Configuration dialog box, on the General tab, select the mode that you want. Your options are:

Interactive Mode	Gives you the option of choosing which updates you want to install
Express Mode	Automatically installs all available updates

4 If you selected Express Mode, select how you want to start checking for updates. Your options are:

I want to press the start button to run LiveUpdate	Gives you the option of cancelling the update
I want LiveUpdate to start automatically	Installs updates automatically whenever you start LiveUpdate

5 To have access to a Symantec self-help Web site in the event that an error occurs while using LiveUpdate, check **Enable Enhanced Error Support**.

6 Click **OK**.

Turn off Express mode

Once you have set LiveUpdate to run in Express mode, you can no longer access the LiveUpdate Configuration dialog box directly from LiveUpdate. You must use the Symantec LiveUpdate control panel.

To turn off Express mode

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Symantec LiveUpdate**.
3. In the LiveUpdate Configuration dialog box, on the General tab, click **Interactive Mode**.
4. Click **OK**.

Run LiveUpdate automatically

You can have LiveUpdate check for protection updates automatically, on a set schedule, by enabling Automatic LiveUpdate. You must continue to run LiveUpdate manually to receive product updates.

Automatic LiveUpdate checks for an Internet connection every five minutes until a connection is found, and then every four hours. If you have an ISDN *router* that is set to automatically connect to your *Internet service provider* (ISP), many connections will be made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate.

To enable Automatic LiveUpdate

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. Set how you want updates to be applied. Your options are:

Apply updates without interrupting me	LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate displays an alert when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
Notify me when updates are available	LiveUpdate checks for protection updates and asks if you want to install them.

3. Click **OK**.

To delete the schedule for Automatic LiveUpdate, disable Automatic LiveUpdate.

To disable Automatic LiveUpdate

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. Click **OK**.

About your subscription

See "About protection updates" on page 170.

Your Symantec product includes a complimentary, limited-time subscription to protection updates that are used by your product. When the subscription is due to expire, you are prompted to renew your subscription.

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates through LiveUpdate or from the Symantec Web site and will not be protected against newly discovered *threats*. Also, whenever you use LiveUpdate, you will receive a warning that your subscription has expired. Follow the on-screen instructions to complete your subscription renewal.

2

Norton AntiVirus

Protecting disks, files, and data from viruses

10

Keeping your computer protected requires regular monitoring by Auto-Protect and Worm Blocking; scanning of your email attachments and files transferred by instant messenger; and frequent system scans. All of these tasks can be set to occur automatically.

For added protection in Norton AntiVirus on Windows 98/98SE/Me, enable Inoculation to alert you if a system file changes.

Ensure that protection settings are enabled

Norton AntiVirus is configured to provide you with complete protection against viruses. It is unlikely that you need to change any settings. However, for maximum protection, you should ensure that your protection features are enabled.

For specific information about a particular option and its protection settings, see the online Help.

This table summarizes the maximum protection settings and where you can find them.

Feature	**In the main window, click**	**Then for maximum protection, select**
Auto-Protect	Enable	On
Email scanning	Options > Email	■ Scan incoming Email ■ Scan outgoing Email If your email program uses one of the supported communications protocols, both options are selected by default.
Timeout protection	Options > Email	Protect against timeouts when scanning Email To prevent connection timeouts while receiving large attachments, enable timeout protection.
Instant messenger scanning	Options > Instant Messenger	Instant messengers that you want to protect
Worm Blocking	Options > Email	■ Enable Worm Blocking ■ Alert me when scanning email attachments
Inoculation (Windows 98)	Options > Inoculation	Inoculate Boot Records

Manually scan disks, folders, and files

If Auto-Protect is enabled and the Norton AntiVirus options are set at their default levels, you normally would not need to scan manually. However, if you temporarily disabled Auto-Protect (for example, to load or use another program that conflicts with Norton AntiVirus), and you forgot to enable it again, it is possible that a virus could be on your hard disk undetected. You can scan your entire computer, or individual floppy disks, drives, folders, or files.

Although the default settings for manual scanning are usually adequate, you can raise the level of Bloodhound heuristics or adjust the options for manual scanning in the Options window.

For more information about manual scanning options, see the online Help.

Perform a full system scan

A full system scan scans all *boot records* and files on your computer.

To perform a full system scan

1. On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
2. In the Scan for Viruses pane, under Task, click **Scan my computer**.
3. Under Actions, click **Scan**.
   When the scan is complete, a scan summary appears.
4. When you are done reviewing the summary, click **Finished**.

Scan individual elements

Occasionally, you may want to scan a particular file, removable drives, a floppy disk, any of your computer's drives, or any folders or files on your computer. You may have been working with floppy disks or have received a compressed file in an email message and suspect a virus. You can scan just a particular disk or individual element that you want to check.

To scan individual elements

1. On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
2. In the Scan for Viruses pane, under Task, select the scan that you want to run.

3 Under Actions, click **Scan**.
If you choose to scan all removable drives or a floppy disk, the scan starts automatically. If you choose to scan drives, folders, or files, a dialog box appears in which you choose which drives, folders, or files to scan.

4 In the dialog box, make your selection, then click **Scan**.
When the scan is complete, a scan summary appears.

5 When you are done reviewing the summary, click **Finished**.

If problems are found during a scan

See "What to do if a virus is found" on page 189.

At the end of a scan, a summary report appears to tell you what Norton AntiVirus found during the scan. If a virus was found and you have requested that Norton AntiVirus repair the file automatically, it is listed as repaired. If the file cannot be repaired, it can be quarantined or deleted.

Create and use custom scans

See "Schedule a custom scan" on page 184.

You can create a custom scan if you regularly scan a particular segment of your computer and don't want to have to specify the segment to be scanned every time. You can also schedule the custom scan to run automatically.

You can delete the scan when it is no longer necessary. For example, if you are working on a project for which you need to frequently swap files with others, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

To create a custom scan

1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.

2 In the Scan for Viruses pane, under Actions, click **New**.

3 In the opening window of the Norton AntiVirus Scan Wizard, click **Next**.

4 Select the items that you want to scan. Your options are:

Add files	Select individual files to be scanned.
Add folders	Select folders and drives to be scanned.

You can use both options to select the combination of items that you want.

5 In the resulting dialog box, select the items that you want to scan.
If you select a folder, all files in that folder are included. If you select a drive, all folders and files on that drive are included.

6 Add the selected items to the list of items to scan by doing one of the following:

- In the Scan Files dialog box, click **Open**.
- In the Scan Folders dialog box, click **Add**.

7 If you need to remove an item from the list, select it, then click **Remove**.

8 When you are done creating the list of items to be scanned, click **Next**.

9 Type a name for the scan by which you can identify it in the list of scans.

10 Click **Finish**.

Run a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

To run a custom scan

1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.

2 In the Scan for Viruses pane, under Task, select the custom scan.

3 Under Actions, click **Scan**.
When the scan is complete, a scan summary appears.

4 When you are done reviewing the summary, click **Finished**.

Delete a custom scan

You can delete custom scans if they are no longer needed.

To delete a custom scan

1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.

2 In the Scan for Viruses pane, under Task, select the custom scan that you want to delete.

If you click the button next to the scan name, the scan runs.

3 Under Actions, click **Delete**.

4 Click **Yes** to verify that you want to delete the scan.

Schedule scans

After installation, Norton AntiVirus automatically runs a weekly full system scan. You can also set up a schedule for custom virus scans.

You can schedule customized virus scans that run unattended on specific dates and times or at periodic intervals. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working.

You cannot schedule the predefined scans in the scan list, but you can schedule any custom scans that you have created.

Schedule a custom scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (such as daily, weekly, or monthly), you are presented with additional fields with which you can refine your request. For example, you can request a daily scan, then schedule it to occur every two days or every three days instead.

To schedule a custom scan

1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.

2 In the Scan for Viruses pane, under Task, select the custom scan that you want to schedule.

If you click the button next to the scan name, the scan runs.

3 Under Schedule Task, click **Schedule**.

4 In the Schedule dialog box, if Show multiple schedules is checked, click **New** to enable the scheduling fields.
If it is not checked, the fields are already enabled.

5 Set the frequency and time at which you want the scan to run.
Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.

6 When you are done, click **OK**.

You can also create multiple schedules for a scan. For example, you could run the same scan at the beginning of your work day and at the end.

To create multiple schedules for a single scan

1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.

2 In the Scan for Viruses pane, under Task, select the custom scan that you want to schedule.

If you click the button next to the scan name, the scan runs.

3 Under Schedule Task, click **Schedule**.

4 In the Schedule dialog box, check **Show multiple schedules**.

5 To set an additional schedule, click **New**.

6. Set the frequency and time at which you want the scan to run.
   Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
7. When you are done, click **OK**.

Edit scheduled scans

You can change the schedule of any scheduled scan, including the weekly full system scan.

To edit a scheduled scan

1. On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
2. In the Scan for Viruses pane, under Task, select the scan that you want to reschedule.

   If you click the button next to the scan name, the scan runs.
3. Under Schedule Task, click **Schedule**.
4. Change the schedule as desired.
5. Click **OK**.

Delete a scan schedule

You can delete any scan schedule. Deleting the schedule does not delete the scan.

To delete a scan schedule

1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.

2 In the Scan for Viruses pane, under Task, select the scan whose schedule you want to delete.

If you click the button next to the scan name, the scan runs.

3 Under Schedule Task, click **Schedule**.

4 In the Schedule dialog box, check **Show multiple schedules**.

5 Select the schedule or schedules that you want to delete.

6 Click **Delete**.

7 Click **OK**.

What to do if a virus is found

11

If after reviewing the information in this chapter, you have not resolved your problem, see “Responding to emergencies” on page 13 and “Troubleshooting” on page 299.

If Norton AntiVirus finds a virus or a file containing a virus or a potential security risk on your computer, there are several possible resolutions to the problem:

- Fix infection
  Removes the virus from the file or if the threat is a worm or Trojan horse, deletes the file.

See “If Norton AntiVirus places files in Quarantine” on page 196.

- Quarantine infection
  Makes the file inaccessible by any programs other than a Symantec antivirus program. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec.
- Delete the file
  Removes the virus from your computer by deleting the file that contains the virus, worm, or Trojan horse. It should be used only if the file cannot be repaired or quarantined.
- Exclude at-risk files
  Excludes the files at risk from future scans. If you exclude a file, you are doing so permanently from future scans. The threat may still be on your computer.

Viruses can be found during a manual or scheduled scan or by Auto-Protect when you perform an action with an infected file. Threats and security risks can appear during an instant messenger session, when sending an email message, or during a manual or scheduled scan.

If a virus is found during a scan

If Norton AntiVirus finds a virus, Trojan horse, worm, or security risk during a scan or from an instant messenger session, you either receive a summary of the automatic repair or deletion results, or use the Repair Wizard to resolve the problem.

Review the repair details

If you have set your manual scan options so that Norton AntiVirus repairs or deletes files automatically, and all infected files could be repaired or deleted, the scan summary lists the number of files found, infected, and repaired or deleted. This information is presented for status purposes only; you don’t need to take further action to protect your computer. If you want to know more, you can check the repair details to see which files were infected and with which *threats*.

To review the repair details

1. In the scanner window, in the Summary pane, click **More Details**.
2. When you are done reviewing the results, click **Finished**.

Use the Repair Wizard

If there are files that could not be fixed, or if you have set options so that Norton AntiVirus asks you what to do when a virus or threat is found, the Repair Wizard opens. If Norton AntiVirus did not attempt a repair, the Repair Wizard opens in the Fix Infection pane. Otherwise, it opens in the Quarantine window.

To use the Repair Wizard

1. If the Repair Wizard opens in the Fix Infections pane, uncheck any files that you don’t want Norton AntiVirus to fix.
   All files are checked by default. This is the recommended action.
2. Click **Fix**.
   If any files cannot be fixed or deleted, the Quarantine Infections window opens. All files are checked to be added to Quarantine by default. This is the recommended action.
3. In the Quarantine window, uncheck any files that you do not want to quarantine.
4. Click **Quarantine**.
   If any files could not be quarantined, the Delete window opens. All files are checked to be deleted by default.
5. In the Delete window, uncheck any files that you do not want to delete.

If you do not delete the infected files, the virus or file at risk remains on your computer and can cause damage or be transmitted to others.

6. Click **Delete**.
   If any files could not be deleted, the Exclude At-risk Files window opens to allow you to exclude files considered to be at risk from future scans.
7. In the Exclude At-risk Files window, select any files that you want to exclude.
8. Click **Exclude**.
9. Once all of the files have been repaired, quarantined, deleted, or excluded, the Scan Summary window opens.

If any files could not be deleted, they appear in the Scan Summary window with a status of at risk or delete failed. There are a variety of reasons why some files cannot be deleted: a file could be in use or part of a larger program. Norton AntiVirus recommends that you select the threat name to review the information from the Internet and determine the appropriate action.

10 When you are done reviewing the summary, click **Finished**.

If a virus is found by Auto-Protect

See "Ensure that protection settings are enabled" on page 179.

Auto-Protect scans files for viruses when you perform an action with them, such as moving them, copying them, or opening them. If it detects a virus or virus-like activity, in most cases you receive an *alert* telling you that a virus was found and repaired. How you proceed depends on the operating system that you are using.

If you are using Windows 98/98SE/Me

If a virus or threat is found and repaired by Auto-Protect in Windows 98/98SE/Me, you receive an *alert* telling you which file was repaired or deleted.

To close the alert

❖ Click **Finish**.

If you have set your options so that Auto-Protect asks you what to do when it finds a virus, the alert asks you to choose one of the following actions. The recommended action is always preselected.

Action	Result
Repair the infected file	Automatically eliminates the virus, Trojan horse, or worm and repairs or deletes the infected file. When a virus is found, Repair is always the best choice.
Quarantine the infected file	Isolates the infected file, but does not remove the threat. Select Quarantine if you suspect that the infection is caused by an unknown threat and you want to submit the threat to Symantec for analysis.

Action	Result
Delete the infected file	Erases both the threat and the infected file. Select Delete if Repair is not successful. Replace the deleted file with the original program file or backup copy. If the virus, Trojan horse, or worm is detected again, your original copy is infected.
Do not open the file, but leave the problem alone	Stops the current operation to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time that you perform the same activity.
Ignore the problem and do not scan this file in the future	Adds the file that is suspected of containing a threat to the Exclusions list. When you add a file to the Exclusions list, the file is excluded from any future virus scans, unless you remove it from the list. Select this option only if you know that the file does not contain a virus.
Ignore the problem and continue with the infected file	Continues the current operation. Select this option only if you are sure that a virus, Trojan horse, or worm is not at work. You will receive an alert again. If you are not sure what to do, select Do not open the file, but leave the problem alone.

If a file cannot be repaired, you receive an alert telling you that the repair was not made and recommending that you quarantine the file. You have the same options as those listed in the table, with the exception of Repair the infected file.

If you are using Windows 2000/XP

If a virus is found and either repaired or automatically deleted by Auto-Protect in Windows 2000/XP, you receive an *alert* telling you which file was repaired or deleted and which virus, Trojan horse, or worm was infecting the file. If you have an active Internet connection, selecting the virus name opens the Symantec Web page that describes the virus.

To close the alert

❖ Click **OK**.

If the file cannot be repaired, you receive two alerts, one telling you that Auto-Protect was unable to repair the file, and another telling you that access to the file was denied.

See "If Norton AntiVirus places files in Quarantine" on page 196.

You can set your Auto-Protect options to try to quarantine any infected files that it cannot repair. If you do this, you are informed if any files are quarantined.

To resolve problems with unrepaired files

1 Run a full system scan on your computer to ensure that no other files are infected.

See "If a virus is found during a scan" on page 190.

2 Follow the recommended actions in the Repair Wizard to protect your computer from the infected files.

If a threat is found by Worm Blocking

See "Ensure that protection settings are enabled" on page 179.

If a program tries to email itself or email a copy of itself, it could be a worm trying to spread via email. A *worm* can send itself or a copy of itself in an email message without any interaction with you.

Worm Blocking continually scans outgoing email attachments for worms. If it detects a worm, you receive an *alert* telling you that a malicious worm was found.

The alert presents you with options and asks you what to do. If you were not sending an email message at that time, then it is probably a worm and you should quarantine the file. You can click Help on the alert for additional information about how to respond.

After you have responded to the *threat* and deleted the file, you could still have an infected system. Follow these procedures.

Procedure	For more information
Run LiveUpdate to ensure that you have the latest protection updates.	See "About protection updates" on page 170.
Scan your system.	See "Perform a full system scan" on page 181.

Procedure	For more information
Go to the Symantec Security Response Web page for the most up-to-date virus definitions and clean-up tools.	See the Symantec Security Response Web page at securityresponse.symantec.com

If Inoculation alerts you about a change in system files

❗ Inoculation protection is available on Windows 98/98SE/Me systems only.

See "Ensure that protection settings are enabled" on page 179.

System files can change for a variety of reasons. You may have updated your operating system or repartitioned your hard disk, or you could have a virus. Norton AntiVirus alerts you when a change occurs in your system files.

If you get an *alert* about a change in your system files, you have two options. You can update your Inoculation snapshot or repair the file. Before you repair the file, be sure that your virus definitions are up-to-date and run a scan.

To respond to Inoculation changes

❖ In the Alert window, select the action that you want to take. Your options are:

Update the saved copy of my Master Boot Record	Use if the alert appears after a legitimate change in system files.
Restore my Master Boot Record	Use if you are certain the system did not change for legitimate reasons.

If Norton AntiVirus places files in Quarantine

Once a file has been placed in Quarantine, you have several options. All of the actions that you take on files in Quarantine must be performed in the Quarantine window.

The toolbar at the top of the Quarantine window contains all of the actions that you can perform on quarantined files.

Add Item	Adds files to Quarantine. Use this action to quarantine a file that you suspect is infected. This action has no effect on files that are already in Quarantine.
Properties	Provides detailed information about the selected file and the virus that is infecting it.
Repair Item	Attempts to repair the selected file. Use this action if you have received new virus definitions since the file was added to Quarantine.
Restore Item	Returns the selected file to its original location without repairing it.
Delete Item	Deletes the selected file from your computer.
Submit Item	Sends the selected file to Symantec. Use this option if you suspect that a file is infected even if Norton AntiVirus did not detect it.
LiveUpdate	Runs LiveUpdate to check for new protection and program updates. Use this if you haven't updated your virus definitions for a while and then try to repair the files in Quarantine.

To open the Quarantine window

1. On the left side of the main window, under Norton AntiVirus, click **Reports**.
2. In the Reports pane, on the Quarantined items line, click **View Report**.

To perform an action on a file in Quarantine

1 In the Quarantine window, select the file on which you want to perform the action.

2 On the toolbar, select the action that you want to perform.

3 When you are finished, on the File menu, click **Exit**.

If Norton AntiVirus cannot repair a file

See "Keeping current with LiveUpdate" on page 169.

One of the most common reasons that Norton AntiVirus cannot automatically repair or delete an infected file is that you do not have the most up-to-date virus definitions. Update your virus definitions with LiveUpdate and scan again.

If that does not work, read the information in the report window to identify the types of items that cannot be repaired, and then take one of the following actions, depending on the file type.

File type	Action
Infected files with .exe, .doc, .dot, or .xls file name extensions (any file can be infected)	Use the Repair Wizard to solve the problem. For more information, see the online Help.
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using the Rescue Disks or your operating system disks. For more information, see the online Help.

Look up viruses on the Symantec Web site

The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions. You must be connected to the Internet to look up viruses.

To look up viruses

1. On the left side of the main window, under Norton AntiVirus, click **Reports**.
2. In the Reports pane, on the Online Virus Encyclopedia line, click **View Report**.
   The Symantec Web site opens in your Internet browser.
3. Use the links on the Web page to access the virus information for which you are looking.

3

Norton Utilities

Finding and fixing problems

12

Trouble-free computing depends on the integrity of your computer, which requires an error-free hard disk and a correctly installed copy of Windows. Although most computers start out this way, over time Windows and hard drives are likely to degrade. This degradation, if not corrected, can ultimately lead to data loss.

Norton SystemWorks includes Norton Utilities tools to monitor your computer for potential problems, examine your disk for directory and disk problems, and diagnose Windows problems.

Norton System Doctor continuously monitors your computer to keep it running at peak efficiency. If directory, disk, or Windows problems occur, you can diagnose and fix these problems quickly using Norton Disk Doctor and Norton WinDoctor.

The CD does not support running Norton Disk Doctor on NTFS *partitions* or FAT16 drives with 64 KB clusters (available in Windows 2000/XP only). If you need support for this capability, install the complete Norton Disk Doctor package on your computer.

About Norton Utilities alerts

See "Monitor your computer's health" on page 203.

When one of the Norton Utilities tools detects a problem with your computer, it displays a message. These messages, which are called *alerts*, may appear when you are running other programs and Norton Utilities detects a problem.

For example, if Norton System Doctor finds a problem, it displays a red light sensor. Alerts do not appear unless you set the sensor properties to Display Alarm Message.

Monitor your computer's health

Norton System Doctor continuously monitors your computer to keep it free of problems and running at peak efficiency. It alerts you immediately when conditions require attention and fixes many problems automatically, without interrupting you.

The Norton System Doctor main window contains a panel of sensors that monitor many aspects of your computer, including the disks, memory, CPU, and network. Norton System Doctor sensors include alarms that alert you to critical conditions that require attention. The sensors also provide information that helps you to fine-tune your computer's performance.

While the default settings are ideal for most users, Norton System Doctor is completely customizable.

See "Use online Help" on page 93.

For more information, see the online Help.

About disk and Windows errors

Trouble-free computing depends on the integrity of your computer. This integrity is based on an error-free hard disk and a correctly installed copy of Windows. Both Windows and your hard disk can develop errors as you use your computer. If they are not corrected, the accumulation of errors can lead to data loss.

See "Monitor your computer's health" on page 203.

The best cure for any problem is prevention. If you keep Norton System Doctor running at all times, it spots problems early and recommends corrective action.

Norton SystemWorks includes several tools that help you identify and repair disk and Windows problems.

One Button Checkup	See "When to use One Button Checkup" on page 204.
Norton System Doctor	See "Monitor your computer's health" on page 203.
Norton Disk Doctor	See "When to use Norton Disk Doctor" on page 204.
Norton WinDoctor	See "When to use Norton WinDoctor" on page 205.

When to use One Button Checkup

Some scans in One Button Checkup provide an alternative to the monitors in Norton System Doctor. Norton System Doctor monitors a wider variety of conditions and remains in your computer memory. One Button Checkup runs scans when you start them manually or when you schedule them. If you have a particular condition that you want to monitor continuously, use Norton System Doctor.

When to use Norton Disk Doctor

Norton System Doctor includes Norton Disk Doctor and Surface Test sensors that notify you when a potential disk problem is detected. Norton Disk Doctor runs automatically to diagnose the problem and make immediate repairs.

Norton Disk Doctor performs several tests on the disk, checking everything from the *partition* table to the physical surface. If Norton Disk Doctor finds a problem, it notifies you before it makes repairs. If you set Norton Disk Doctor to automatically fix errors, repairs are made automatically. After it diagnoses and repairs a disk, Norton Disk Doctor displays a report that lists the problems that were found, the problems that were fixed, and the areas of the disk that are problem-free.

You can run Norton Disk Doctor and examine your disk from the program CD.

When not to use Norton Disk Doctor

Do not run the *DOS* version of Norton Disk Doctor on partitions that were created with Linux FDISK or Disk Druid. If you choose to fix errors on partitions that were created with these utilities, it is critical that you make an Undo file.

See "Create an Undo file to reverse repairs" on page 207.

See "Create and use Rescue Disks" on page 86.

Use Norton Disk Doctor to fix an invalid partition only if it is completely inaccessible from Windows or DOS. Update your Rescue Disks prior to any kind of partition repair operation.

Norton Disk Doctor can only revive FAT or FAT32 partitions on computers that are running Windows 2000/ XP. It cannot revive NTFS partitions.

To repair corrupted *boot records*, use the DOS version of Norton Disk Doctor; do not use the Windows version. The Windows version diagnoses the problem, but it will not repair the boot record as well as the DOS version of Norton Disk Doctor.

When to use Norton WinDoctor

Norton WinDoctor is the safe and easy way to diagnose and repair common Windows problems. It checks the necessary information for Windows to run properly and checks for components that are needed by programs that run in Windows.

Combined with Norton System Doctor, Norton WinDoctor can automatically monitor your computer for Windows problems. If a problem is detected, Norton System Doctor alerts you to start Norton WinDoctor to correct it.

See "Start utilities from the CD" on page 68.

You can run Norton WinDoctor and other utilities from the program CD.

Check your disk with Norton Disk Doctor

Run Norton Disk Doctor often to keep your hard disk free of accumulated errors.

Running Speed Disk frequently will improve the performance of the scans that Norton Disk Doctor conducts. However, if you suspect that your disk has problems, do not run Speed Disk until you have corrected them with Norton Disk Doctor.

To perform a disk check

1 On the left side of the main window, click **Norton Utilities** > **Find and Fix Problems**.

2 Click **Norton Disk Doctor**.

3 In the Norton Disk Doctor window, select one or more drives to diagnose.

4 If you want Norton Disk Doctor to repair problems automatically without stopping to describe them to you, check **Automatically fix errors**.

See "Customize Norton Disk Doctor" on page 210.

5 If you want to specify which tests Norton Disk Doctor runs and other options, click **Options** and set the options that you want.
Norton Disk Doctor run-time options are different depending on whether your computer is running Windows 98/Me or Windows 2000/XP.

6 Click **Diagnose**.
Norton Disk Doctor restarts its diagnosis if it detects that another program is writing to the examined disk. Restarting ensures the integrity of the data on the disk if repairs are required. Restarting may occur

several times during a single Norton Disk Doctor session.

7 Follow the on-screen instructions as Norton Disk Doctor identifies and fixes any problems.

8 When the diagnosis and repairs are complete, click **Close**.

Run Norton Disk Doctor in the background

In Windows 98/Me, you can run Norton Disk Doctor in the background while you work by minimizing it after you click Diagnose. When Norton Disk Doctor detects a pause in disk activity, it begins diagnosing the disk. (In Windows 98/Me, one of the Norton Disk Doctor advanced options lets you specify how long a pause is required.)

See "Monitor your computer's health" on page 203.

Norton Disk Doctor diagnoses your disk only once each time that it is run minimized. To continuously test the integrity of your disk, use Norton System Doctor. The Disk Doctor and Surface Test sensors can monitor your disk while you work. When problems are detected, Norton System Doctor can run Norton Disk Doctor immediately.

Create an Undo file to reverse repairs

In Windows 98/Me, Norton Disk Doctor gives you the option of creating an Undo file before it makes disk repairs. In the unlikely event that you need to reverse the changes made by Norton Disk Doctor, you can use the Undo file to return your disk to the state that it was in prior to the repairs.

If you do not want Norton Disk Doctor to create an Undo file, you can uncheck the Undo File option in the Custom Repair Options dialog box. Turn off the undo prompts only if you are certain that you will not need to undo the repairs.

To create an Undo file in Windows 98/Me

See "Check your disk with Norton Disk Doctor" on page 206.

1. Start Norton Disk Doctor and examine a disk.
   When Norton Disk Doctor finds a problem that must be repaired, it describes the problem and asks if you want to save an Undo file.
2. In response to the Norton Disk Doctor prompt, click **Create Undo File**.
3. In the Select Undo Location dialog box, select a drive on which to create the Undo file, then click **Create**.
4. Follow the on-screen instructions to finish creating the Undo file.

You should inspect any data files that were affected by the repairs (they are indicated in the Norton Disk Doctor report). If you are not satisfied with the results of the repair, click **Undo** immediately. You should not try to undo the changes if you have saved, deleted, or copied files following the repairs. Attempting to do so may result in a loss of data.

If you need to reverse a repair

You can reverse a previously made disk repair if you authorized Norton Disk Doctor to create an Undo file when the previous examination was made.

If you have copied, saved, or deleted files on your disk after making repairs with Norton Disk Doctor, do not attempt to undo the repairs. Changes to the file system after the repairs invalidate the Undo file data. Attempting to undo repairs after you have changed files on your disk can result in lost or damaged data. Also, do not attempt to undo changes if Norton Disk Doctor reported any disk surface errors.

To undo Norton Disk Doctor repairs in Windows 98/Me

1. On the left side of the main window, click **Norton Utilities** > **Find and Fix Problems**.
2. Click **Norton Disk Doctor**.
3. In the Norton Disk Doctor window, click **Undo**.
4. Read the confirmation message.

5. If you still want to attempt to undo your repairs, click **Continue**.
6. Select the drive that contains the Undo file, then click **OK**.
7. Verify that the undo information was created at the expected date and time, then click **Yes**.

Create a Norton Disk Doctor report

When Norton Disk Doctor finishes testing your disk for errors, it displays a summary of test results, which include any problems that were found, and whether repairs were made.

You can also view and print a report that includes detailed information about the examined disk and the repairs that were made. The detailed report can help you track recurring disk problems.

The Norton Disk Doctor report is not available if you are using a version of Norton Utilities that is in a different language than your operating system.

To create a Norton Disk Doctor report

See "Check your disk with Norton Disk Doctor" on page 206.

1. Examine a disk with Norton Disk Doctor.
2. In the Test Results dialog box, click **Details**.
3. Click **Print**.
4. Specify the output type for the test results. Your options are:

Print to Printer	Print the report to the printer that you select. To specify printer options, click the open folder icon.
Print to File	Save the test results in a text file with the name and location that you specify. To specify a file name, click the open folder icon.

Types of Norton Disk Doctor tests

Norton Disk Doctor checks your disk's physical surface for abnormalities that would affect the data storage on your disk. Norton Disk Doctor moves any data that it can from damaged areas of the disk to undamaged areas. It also marks the damaged areas so that your computer won't attempt to store data there in the future.

See "Use online Help" on page 93.

For more information, see the online Help.

Customize Norton Disk Doctor

In Norton Disk Doctor you can customize how repairs are handled, if Norton Disk Doctor runs a disk check on startup, its appearance during disk examinations, how thoroughly it should examine a disk, and what tests should be run or skipped.

In Windows 2000/XP, most options are built in and are not configurable.

To customize Norton Disk Doctor

1. On the left side of the main window, click **Norton Utilities > Find and Fix Problems**.
2. Click **Norton Disk Doctor**.
3. In the Norton Disk Doctor main window, click **Options**.
4. Click a tab to adjust the associated options.

   See "Use online Help" on page 93.

   For more information, see the online Help.
5. When you're finished, click **OK**.

Find and fix Windows problems

Norton WinDoctor diagnoses and repairs the most common types of Windows problems. You can tailor the repair process to your own needs by selecting which tests to run and which problems to fix.

Norton WinDoctor does the following:

- Inspects everything that's required for Windows to run properly, and keeps Windows running at peak efficiency.
- Checks for components that are needed by the programs that you run in Windows.
- Displays an easy-to-read report that lists the problems that it found, the problems that it fixed, and the severity of each problem.
- Lets you tailor the repair process. You can specify which problems to fix and how to fix them. Or, you can choose to fix all of the found problems automatically and let Norton WinDoctor take care of everything.

Run Norton WinDoctor when you receive a Windows problem alert, or run it regularly to keep your Windows operating system free of accumulated errors.

To find and fix Windows problems

1. On the left side of the main window, click **Norton Utilities** > **Find and Fix Problems**.
2. Click **Norton WinDoctor**.
3. Select an action to perform. Your options are:

Perform all Norton WinDoctor tests	Performs all available scans without further interruption.
Let me choose which tests to run	Displays a list of scans that you can exclude or include. See "Select Norton WinDoctor scans" on page 213.
View Repair History and (optionally) undo changes	Lets you review and reverse Norton WinDoctor's previous repairs. For more information, see the online Help.

4. Click **Next**.
5. When the scan is finished, click **Next**.

6 To see the list of problems, click **Finish**.
Norton WinDoctor displays a list of problems found, organized by problem type and severity.

7 Do one of the following:

Click **Repair All.**	Repair all problems automatically. See "To use Automated Repair" on page 216.
Select a problem or group of problems, then click **Repair.**	Repair a specific problem or group of problems. For more information, see the online Help.
Sort the list of problems.	For more information, see the online Help.
Ignore problems.	For more information, see the online Help.

8 When the repairs are finished, click **OK**.

9 Close the Norton WinDoctor window.

Create a Norton WinDoctor log file

Norton WinDoctor can create a log file of all the changes made to Windows during a repair session. The log file is not the same as the Repair History, which you can use to review and reverse repairs.

To have Norton WinDoctor create a log file

See "Find and fix Windows problems" on page 210.

1 Run Norton WinDoctor.

2 With the Norton WinDoctor Problems Found dialog box open, press **Ctrl+Alt+S**.

3 In the Save dialog box, specify the destination and file name.
The log file is formatted as a text file.

4 Click **Save**.

Select Norton WinDoctor scans

Norton WinDoctor can perform a variety of scans to find problems with your system. You may not wish to run every scan every time you run Norton WinDoctor. When you start Norton WinDoctor, the program displays a list of available scans and allows you to select the ones that you want Norton WinDoctor to run.

See "To select WinDoctor Analysis Agents" on page 214.

WinDoctor Analysis Agents provide filtering for the problems found during scans. They eliminate some common problems, and provide additional repair options.

To select Norton WinDoctor scans

See "Find and fix Windows problems" on page 210.

1. Run Norton WinDoctor.
2. In the Norton WinDoctor wizard, click **Let me choose which tests to run**, then click **Next**.

See "To select WinDoctor Analysis Agents" on page 214.

3. To specify how you want Norton WinDoctor to process the problems that it finds, select Analysis Agents.
4. Check the scans that you want to run. Your options are:

Windows Registry Sections	These scans examine the following sections of the Windows Registry: - ActiveX/Come - ActiveX/COM SubKey - Application Paths - Device Drivers - Fonts - Help - Microsoft Shared - Run - Sound Customization - Symantec Shared - Uninstall

Program Integrity	Scans the Windows Desktop, Start menu, application paths, and the shared .DLL and Uninstall sections of the Windows Registry for invalid entries.
Shortcuts	This scan checks that any program shortcuts (.PIF and .LNK files) have valid links to their programs.

To see information about any scan, place your cursor over it and read the tooltip.

5 Click **Next**.

6 Continue with the Norton WinDoctor scan and repair.

7 When the repairs are finished, click **OK**.

8 Close the Norton WinDoctor window.

To select WinDoctor Analysis Agents

See "Find and fix Windows problems" on page 210.

1 Run Norton WinDoctor.

2 In the Norton WinDoctor wizard, click **Let me choose which tests to run**, then click **Next**.

3 Click **Analysis Agents**. Your options are:

Add manual registry editing solution	This agent adds a solution that lets you edit any Windows Registry problems directly from the WinDoctor Problems Found dialog box.
Search Norton Protected Recycle Bin for missing files	This agent includes the Norton Protected Recycle Bin in searches for missing files, and adds an UnErase file recovery option to the list of available repairs.
Search Recycle Bin for missing files	This agent includes the Windows Standard Recycle Bin in searches for missing files, and adds an UnErase file recovery option to the list of available repairs.
Search all hard drives for missing files	This agent attempts to find missing files by searching all local drives for a file with the same name. If a file is found, the repair option lets you link the shortcut to the file.
Detect drive letter changes	This agent checks to see if any problems are due to a change in drive letter assignment. If so, it provides a solution to include the new drive letter.

Detect directories that have moved	This agent checks to see if any problems are due to a directory changing from one drive to another. If so, it provides a solution to include the new drive letter.
Ignore missing files on removable drives	This agent checks to see if any missing file problems are due to files that are located on removable drives. If so, it removes the problem from the list.

To see information about an Analysis Agent, place your cursor over the agent name and read the description that appears in a tooltip.

4 Uncheck one or more problem Analysis Agents, then click **OK**.

5 Continue the scan process.

Select Norton WinDoctor repair solutions

Norton WinDoctor lets you tailor the repair process to your needs. You can specify which problems to fix and how to fix them, or you can let Norton WinDoctor fix all of the found problems automatically.

If you decide that you don’t like a repair that Norton WinDoctor has made, you can undo it. To undo repairs that you made in previous sessions, use Norton WinDoctor’s Repair History feature.

You can use the interactive Automated Repair process, which displays one sub-problem at a time, and presents the available solution methods to repair it. The first solution in the list is the most complete fix for the problem. You may select other solutions or accept the recommendation.

See “Find and fix Windows problems” on page 210.

To use Automated Repair

1. Run Norton WinDoctor.
2. With the Norton WinDoctor Problems Found dialog box open, select solutions to the listed problems. Your options are:

Select Solution list	Select the solution that you want to apply to the problem.
Repair	Click Repair to apply the selected solution.
Cancel	If you selected a problem type with multiple sub-problems, or a group of sub-problems, Cancel allows you to skip the currently displayed sub-problem and display the next one, or close this dialog box.

3. Continue selecting problems and repairing them until you are finished.
4. When the repairs are finished, click **OK**.
5. Close the Norton WinDoctor window.

About problem severity

Norton WinDoctor displays an easy-to-read report of the problems that it found. Problems are listed by problem type in the order of severity.

There are three levels of severity:

Low	A problem that is unlikely to affect your use of the computer, but should be repaired to keep your system uncluttered. For example, you may have a reference to a file in the registry that has been moved or deleted.
Medium	A problem that would be an annoyance to you, but probably won't interfere with the most important tasks that you perform. For example, if an application shortcut refers to a file that is missing or has been moved, you would not be able to launch that application from the shortcut.
High	A problem that can block you from using your computer or could result in data loss. For example, if a file that is required to run an application is missing or corrupt.

Recovering missing or erased files

13

⚠ Do not use UnErase if you purchased Norton SystemWorks to recover files or because you suspect that your computer is infected with a virus. Before you proceed, read the emergency procedures.
See "Responding to emergencies" on page 13.

When you erase a file using Windows Explorer, Windows keeps a temporary copy of the file in the Recycle Bin. However, Windows does not detect files that were erased or overwritten by applications that are running in Windows, erased from a command prompt, or deleted using a permanent method, such as using Shift+Delete.

⚠ If you are unsuccessful in recovering a file using the Norton Protected Recycle Bin or the UnErase Wizard and you have Norton GoBack installed, consider using Norton GoBack to revert your disk to an earlier state when you knew the file existed.

See "Reverting your hard disk" on page 145.

About Norton Protection

The Norton Protected Recycle Bin protects the following types of files:

- Files that are deleted while you are using the command line
- Files that are created and deleted by Windows applications

- Older versions of files that you modify and overwrite
- If the standard Windows Recycle Bin is not enabled, Norton Protection also protects files that would otherwise be under Recycle Bin protection

Files that are shared on a network or stored on a network server and files that were deleted while you were using your computer in DOS mode rather than Windows are not protected.

The Windows 2000/XP operating systems only track ownership and rights on NTFS volumes. With NTFS volumes, you are told how many files are yours before you purge them. If you delete a file on a FAT/FAT32 drive, the system does not differentiate between your files and those belonging to another user. When you purge your files, the system also purges all the files to which the other user has access, which includes all files on FAT/FAT32 volumes.

About UnErase Wizard

UnErase Wizard helps you recover deleted files from the Norton Protected Recycle Bin. In Windows 98/Me, UnErase Wizard can also help you restore files that were unprotected by Norton Protection. Windows 2000/XP can only recover files that were deleted while Norton Protection was turned on.

UnErase Wizard also helps you recover files that are deleted from the standard Windows Recycle Bin, or Novell's Salvage (for recovery of files on a network). In Windows 98/Me, UnErase Wizard frequently recovers unprotected files as well, even those that were deleted from the Recycle Bin.

If you have a dual boot system and the volume that contains deleted files is not NTFS, you can use UnErase Wizard in Windows 98/Me to recover deleted files.

See “Recover a file with UnErase Wizard” on page 221.

Using UnErase Wizard, you can search for a deleted file by its file name and by words that you think the file may contain. This is especially useful if you can’t remember the file name, but you do remember its contents.

Don't use UnErase Wizard to recover and overwrite files that have existing copies in use by either the system or running applications. Examples include SYSTEM.DAT, USER.DAT, applications' registry (.DAT) files, and any applications or DLLs in the Windows System folder.

In many cases, Norton Protection saves files that are overwritten with newer versions. This lets you retrieve earlier versions of the overwritten files.

Recover a file with UnErase Wizard

In Windows 98/Me, installing Norton SystemWorks can overwrite erased files on your hard disk. If you want to try to recover erased files before you install, you should run UnErase Wizard from the program CD. See "When to run disk utilities from the CD" on page 20.

UnErase Wizard displays a list of deleted files or the files that conform to file name criteria that you provide. Each file is described by its name, original location, the date it was deleted, *file type*, file size, and the program that was used to delete it. You can view the contents of a file before or after you recover it.

On Windows 2000/XP, deleted files are not recoverable if they were excluded from Norton Protection and deleted, or if they were protected but deleted from the Recycle Bin before you used UnErase Wizard.

To recover a file with UnErase Wizard

1. On the left side of the main window, click **Norton Utilities** > **Find and Fix Problems**.
2. Click **UnErase Wizard**.
   In the UnErase Wizard dialog box, depending on your operating system, the default selections are:

Find recently deleted files (Windows 98/Me default)	Searches for the names of the most recently deleted files and displays up to a maximum of 25 deleted files. It's best to try this option first.
Find all protected files on local drives (Windows 2000/XP default)	Searches for and displays the names of all of the deleted files that are protected by Norton Protection or the Windows Recycle Bin on your computer.
Find any recoverable files matching your criteria	Prompts you for search criteria. Use this option if you are looking for words that are contained in a deleted file.
Find all Norton Protected Users files (Windows 2000/XP only)	Searches for other users' protected files as well as your own.

3. Do one of the following:
   - To accept the default selection, click **Next**.
   - Select another option, then click **Next**.
4. Click **Next**.
   UnErase Wizard displays a list of the most recently deleted files.
5. If you are using Windows 98/Me and your deleted file is not listed, click **Next**.
   UnErase Wizard guides you through the process of creating a more complete list of deleted files from which to select.
   For more information, see the online Help.
6. Select the file that you want to recover.

7. Click **Recover**.
   If you want to examine the recovered file, make a note of the recovery destination.
8. To close UnErase Wizard, click **Finish**.

A recovered file's name might have a question mark (?) in place of the first letter. If so, you are prompted to type the first letter of the original file name. If you do not know what it is, type any letter from A to Z as a substitute. Make a note of the file name so that you can find it later.

If you delete a file on a floppy disk from a DOS prompt by specifying file name letters after a wildcard (such as DEL *ILENAME.TXT as opposed to DEL FILENAME.TXT or DEL *.TXT), the file is listed as unrecoverable on the Recently Deleted Files page.

To see if a file is recoverable

1. In the center of the file list, right-click, then click **Show Unrecoverable Files**.
2. Click **Next**.
   Use the UnErase Wizard to search for and recover the files.

Improving a computer's performance

14

Your computer's hard disk stores all of your files, applications, and the Windows operating system. Over time, the bits of information that make up your files are spread over the disk. This is known as fragmentation. The more that you use your computer, the more fragmented it gets. Before long, a fragmented hard disk can cause the entire system to slow down.

Speed Disk defragments the bits of information on your hard disk and rearranges them for greatest efficiency in a process called optimization.

About Speed Disk

Speed Disk optimizes an entire disk's files, directories, the MFT, swap file, and security metadata. You can optimize without restarting your computer and optimize in only one pass, even after you optimize the swap file. Intelligent analysis places *file types* in the optimal order for best performance, which reduces the frequency and necessity for substantial reoptimizations.

Use the Disk Optimization sensor in Norton System Doctor to monitor your disks' fragmentation levels. When disks become too *fragmented*, Norton System Doctor can notify you to run Speed Disk.

Why performance degrades

A hard disk is a set of stacked disks onto which data is recorded in concentric tracks. A disk head is like a phonograph arm but in a more fixed position. As the disk spins, two disk heads (one on each side of the disk) write to or read the information on the tracks. How and where your data is organized on your disks affects your computer's performance.

All of your files, applications, and the Windows operating system are stored on your computer's disks. Over time, the bits of information that make up your files gets distributed all over the disk. This is known as *fragmentation*. Fragmentation creates inefficient conditions when you want to store and retrieve information on or from a disk. The more that you use your computer, the worse it gets. A fragmented disk can cause the entire computer to slow down.

Over time, fragments of a file may be scattered in different areas of the disk, away from the original location of the file. These multiple file fragments are tracked in the disk catalog, or Master File Table (MFT), which also grows with the addition of location information.

How fragmentation is calculated

In Windows 2000/XP, the fragmentation level is determined by the formula [total file fragments]/[number of files], expressed as a percentage. Unfragmented files are counted as single *fragments*. You may also see different statistical reporting with Executive Software's Diskeeper, or Disk Defragmenter, the utility that is included with Microsoft Windows.

In Windows 98/Me, Speed Disk compares the number of fragments against the number of files using the formula (Tf / F) * 100 where Tf is the number of file fragments and F is the number of total files. For example, on a disk with 100 files, with one file consisting of 17 fragments, Speed Disk will report that 17 percent of the disk is fragmented. Speed Disk also defragments the swap file and includes it in its calculations.

How fragmentation affects performance

The data storage space on a disk is divided into discrete units called clusters. When files are written to the disk, they are broken up into cluster-sized pieces. When all of the pieces of a file are located in adjacent or contiguous clusters, the file can be accessed quickly because all of the information is in one place.

When files are saved or copied to a disk, there is no discrimination among types of files. On an unoptimized disk, all *file types*, including applications, .dlls, and data files, are intermingled.

When a fragmented file is accessed, disk performance is slower because the drive head must do more work to locate, load, save, and keep track of all of the *fragments* of the file. If free space is also fragmented, the disk head may have to hunt for adequate free space to store temporary files or newly added files.

Free space fragments that are smaller than 16 clusters cannot be used by the Windows 2000/XP File System so these fragments waste drive space. If there is substantial fragmentation on the drive, unavailable free space can consume a lot of potential drive space.

Fragmentation also affects video and other multimedia performance. For example, if a multimedia file such as a movie is being played, and the movie file is fragmented, the player may have to wait for the disk head to locate the next fragment to load.

Speed Disk optimizes fragmented files by rearranging file fragments into adjacent or contiguous clusters. When the disk head can access all of the file data in one location, the file is read into memory faster.

About file fragmentation

The space on a drive is divided into discrete units for allocating file space. The Windows 2000/XP NTFS file system uses *clusters* as its smallest allocation unit. When files are stored to the drive, they are broken up into cluster-size pieces that are tracked in a disk catalog. Cluster sizes vary depending on the overall size of the drive.

Cluster allocation size	Drive size
512 bytes	<512 MB
1024 bytes	512 MB to 1 GB
2048 bytes	1 GB to 2 GB
4096 bytes up to 128 KB	>2 GB

Speed Disk also creates contiguous free space on the disk, which improves system performance when you add new files. This is especially helpful under low disk space conditions where free space fragmentation can cause newly added large files to be fragmented from the start.

Differences between optimization and defragmentation

The terms defragmentation and optimization are often used interchangeably, but they are not the same.

Defragmentation is the process of rearranging the way that files are organized on a disk so that the data that comprises each file is stored in adjacent or contiguous disk clusters.

Optimization maximizes the usable free space on a disk by grouping files based on how they are accessed. The most frequently used files are placed at the beginning of the disk for fast access. Infrequently used files are placed out of the way. Free space is consolidated to avoid fragmenting newly added files, and extra space is added after major data structures so that they can grow without immediately becoming fragmented again.

Before you optimize your disks

Before you run Speed Disk, prepare your computer for optimization. This includes ensuring that your disk has no errors by running Norton Disk Doctor, deleting temporary files, completing any major software installations or removals, backing up your files, closing all programs, and setting the Speed Disk options that are appropriate for your computer.

If you are optimizing for the first time

See "Specify file placement during optimization" on page 240.

A disk's first optimization may take significantly longer than subsequent optimizations because Speed Disk must move the files and free space in a particular order. After a disk has been optimized, only new and expanded files need optimization.

See "Customize Speed Disk" on page 239.

If optimization is taking too much time, or using too many computer resources, you may want to adjust the Speed Disk options.

The benefits of optimization, which include faster access and improved overall performance, make the initial optimization time worthwhile. Speed Disk takes advantage of improvements that were made in the first optimization to reduce subsequent optimization times.

If you are optimizing NTFS volumes

If you are optimizing NTFS volumes, you should select the Global option, "Scan for errors before optimizing." This causes Speed Disk to check the integrity of the volume before you proceed. If the selected disk is a FAT volume, a message informs you that Norton Disk Doctor should be run before the optimization.

Prepare your computer

Before you run Speed Disk, you need to prepare your computer.

Step	For more information
Back up your files.	Refer to your system documentation.
Delete temporary files.	Refer to your system documentation.
Complete any program installations or uninstallations.	See "If you are optimizing for the first time" on page 229. For any special considerations, refer to your system documentation.
Run Norton Disk Doctor or CHKDSK.	See "If you are optimizing NTFS volumes" on page 229.
Analyze disk fragmentation (Windows 2000/XP).	See "Analyze disk fragmentation" on page 237.
Set Speed Disk options.	See "Customize Speed Disk" on page 239.
Close all programs (Windows 98/Me).	Refer to your system documentation.

Optimize your hard disks

If you followed the suggestions in "Before you optimize your disks" on page 229, you are ready to optimize a disk for the first time. Windows 98/Me optimization procedures are different than Windows 2000/XP procedures.

On disks with more than 6000 folders or folders with more than 2000 large files (files that are larger than 5 MB), the initial Speed Disk scan will run very slowly and may even appear to stop. You should always allow the scan to complete.

About the phases of optimization

Speed Disk goes through the following phases in the course of optimization:

Scan for errors before optimizing NTFS volumes (optional)	When this setting in the Global Options is turned on (the default setting is off), Speed Disk runs a brief check of the disk for any problems.
Scanning	Speed Disk scans the entire hard disk and gathers information about how many files of each file type are present, the amount of empty space, and the number of partially used clusters. Gathering data on file fragmentation and unmovable files can take some time, depending on the size of the volume, the number of files on the volume, and the degree of file fragmentation. Unmovable files are shown in the optimization map after the drive is scanned in the first phase of optimization. However, to save time, the map does not show fragmented or unmovable files until after Speed Disk performs a fragmentation analysis.
Sorting	Speed Disk sorts the files according to their types. See "File placement during optimization" on page 231.
Moving	Speed Disk moves the files into the areas of the drive that are assigned to their types. See "File placement during optimization" on page 231.

File placement during optimization

Speed Disk places files in order, from the beginning of the drive to the end of the drive. In general, the default settings will provide the best performance. You should change the default settings only if your files require special consideration. File types are placed in the following order.

Drive order	File type
Start	Master File Table (MFT)
2	Files in the Files First list in Drive Options
3	Paging File
4	Directories
5	Files that were accessed in the last two months
6	Files that were optimized by Speed Disk
7	Files that were modified within the last two to four months
8	Files that were modified within the last two months
9	Files that were not accessed in the last two months
10	Files that were not modified in the last four months
11	Files in the Files Last list in Drive Options
12	Optimized free space
--	Extra space placed after the data files to allow for growth
--	Files and other disk data not yet optimized
13	Files in the Files At End list in Drive Options

Optimize a disk

In Windows 98/Me, Speed Disk checks the disk for errors before optimization proceeds.

To optimize a disk in Windows 2000/XP

1. On the left side of the main window, click **Norton Utilities** > **Optimize Performance**.
2. Click **Speed Disk**.

3 In the Speed Disk dialog box, under Select a Drive, select the disk that you want to optimize (the default disk is C).

4 Under Select a View, select the options that you want. Your options are:

Optimization Map	Lets you optimize disks. When optimization starts, the drive map shows how Speed Disk organizes file types, which are colored according to the legend. See "About the optimization map" on page 235.
Analysis	Lets you generate statistics about a selected disk. See "Analyze disk fragmentation" on page 237.
Drive Options	Lets you customize file placement on a disk. See "Customize Speed Disk" on page 239.
Schedule Options	Lets you set an optimization schedule for each disk. See "Schedule optimization" on page 240.

See "About the optimization map" on page 235.

5 Under Legend, view and customize the colors that are associated with file types on the disk map, and with segments in the analysis pie charts.

6 Click **Start Optimizing**.
Once optimization has started, you can quit Speed Disk, and optimization continues in the background.

7 If you want to optimize additional disks, select another disk in the list, then click **Start Optimizing**.
The recommended number of concurrent optimizations is 2.

To optimize a disk in Windows 98/Me

1 On the left side of the main window, click **Norton Utilities** > **Optimize Performance**.

2 Click **Speed Disk**.

3 In the Speed Disk dialog box, under Select a Drive, select the disk that you want to optimize (the default disk is C).
Speed Disk scans the disk and makes a recommendation based on the current fragmentation.

4 Select an optimization option. Your options are:

Full Optimization	Defragments and optimizes the files and consolidates the free disk space to one area on the disk. This method gives the best results, but takes the longest. If you select this method, you can also customize how the optimization is performed.
Unfragment Files Only	Optimizes as many files as possible without consolidating the free disk space. This method is faster than a full optimization, but may not optimize as many files as efficiently. Some large files may not be optimized at all.
Unfragment Free Space	Quickly consolidates the free space to one area of the disk, but does not optimize any files. Use this method before you install new software or create a compressed volume if you don't have time for a full optimization.

5 Ensure that **Optimize Swap file** is checked.
Unchecking this option is not recommended.

6 When prompted, disable the Microsoft Task Scheduler.
If the Microsoft Task Scheduler is enabled, Speed Disk performance might be forced to restart many times.

7. Click **Start**.
   You can view Speed Disk progress on the optimization map.
   When Speed Disk has finished optimizing, a message appears.
8. Click **OK**.
9. Close the Speed Disk window.

Run Speed Disk in the background

You can run Speed Disk efficiently in the background while you work by minimizing it after you start the optimization. When Speed Disk detects a pause in disk activity, it begins optimizing the disk.

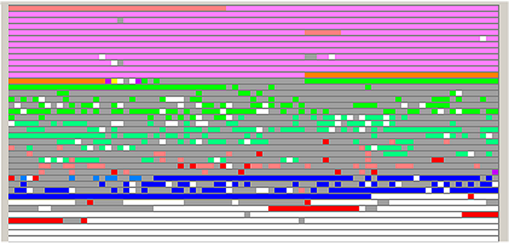
You can specify how long a pause in disk activity is necessary before Speed Disk begins optimizing in the background. You can also configure Speed Disk to wait for a specified time period of communication port inactivity before you begin background optimizations. If you are using fax software to send and receive faxes, you should enable this feature to avoid conflicts between the fax software and Speed Disk.

If you schedule concurrent optimizations of multiple disks, you can minimize the effect on programs that are running in the foreground.

Norton System Doctor includes the Disk Optimization sensor, which can automatically monitor a disk while you work and notify you when the files become too fragmented. You can configure Norton System Doctor to run Speed Disk automatically when fragmentation exceeds a specified value.

About the optimization map

The optimization map is a graphical representation of the files that are arranged on a disk. The customizable color-coding helps you identify how efficiently disk space is being used. Each block on the map represents a number of clusters on the drive.



On the optimization map, you may see small blocks of extra space mixed in with optimized files, even after Speed Disk has optimized a disk. Speed Disk adds extra space after each category of optimized files to allow for future growth. This allows categories of files to expand without causing immediate fragmentation and extends the benefits of optimization.

In Windows 98/Me, you can click any block in the disk map to display information about the block location, files that occupy that cluster, and whether a file is fragmented, optimized, or unmovable.

If you select a file in the list, all the blocks that contain any portion of the file are highlighted in the disk map.

See "Use online Help" on page 93.

For more information about the optimization map, see the online Help.

About the Analysis View

In Windows 2000/XP, Speed Disk displays an analysis of each drive so that you can determine its fragmentation level, and if necessary, determine if any special action is required for recurring fragmented files.

The Analysis View displays file fragmentation, free space fragmentation, and general disk utilization. The lower part of the view lists the most fragmented files with the number of *fragments*.

Analyze disk fragmentation

In Windows 2000/XP, you can use Speed Disk to perform an analysis of each disk to determine its fragmentation level before you optimize it.

You can use the Analysis View to identify the most fragmented files. You can then use that information to reduce susceptibility to repeated fragmentation. After you run the analysis, any highly fragmented files are listed in the Most Fragmented Files list. By specifying the placement of highly fragmented files, you can reduce the amount of fragmentation that occurs during use.

See "Customize Speed Disk" on page 239.

If these files become fragmented frequently, even following optimization, you can use the Speed Disk Drive Options to specify where you want Speed Disk to place the files during the next optimization.

To analyze a disk's fragmentation in Windows 2000/XP

1. In the Speed Disk main window, under Select a Drive, select the disk that you want to analyze (the default disk is C).
2. Under Select a View, click **Analyze**.
3. In the Speed Disk main window, click **Actions**.
4. Click **Start Analyzing**.
   The analysis time depends on the degree of fragmentation, the size of the disk, and the number of files on the disk.

5 If you want to analyze additional disks, select another disk in the list, then click **Start Analyzing**.

6 To stop the analysis, click **Stop Analyzing**.

7 Close the Speed Disk window.

Speed Disk provides the following statistics to help you determine an optimization strategy:

Bytes used	The total number of bytes occupied by files or file fragments on the disk
Bytes free	The total bytes of free space on the disk
Percent of Disk Used	The percentage of occupied disk space
Number of Folders	The total number of folders on the disk
Number of Files	The total number of files on the disk

View file fragmentation in Windows 98/Me

In Windows 98/Me you can view a fragmentation report that shows fragmentation for individual files.

To view a fragmentation report in Windows 98/Me

1 In the Speed Disk window, click **Properties** > **Fragmentation Report**.

2 In the Fragmentation Report window, in the left pane, select a folder.
The list of files that are inside of the selected folder shows the following:

- File name
- Percent optimized (100% means that the file is unfragmented)
- Number of file fragments, if any
- Number of clusters that the file occupies

Customize Speed Disk

During optimization, Speed Disk places files in the best locations for efficient access and flexible growth. However, there may be situations in which you need to ensure that certain files are placed in specific areas on the disk, so that they are accessed first or have room to expand without becoming fragmented.

Speed Disk provides options that let you customize the following aspects of the disk optimization process:

- Schedule optimizations for individual volumes that are based on time or threshold of fragmentation.
- Adjust the system resources that are used by Speed Disk in relation to other running processes.
- Customize the optimization for each disk.
- Run Speed Disk in the background to optimize volumes at preset times.
- Record optimization events to the system Event Log.

Speed Disk stores the optimization options that you choose for each disk, so you do not need to reset options each time that you optimize unless you want to change them.

Speed Disk options determine how Speed Disk optimizes specific disks. For example, if one disk contains mostly data and another contains a combination of data and frequently used applications, you may want to specify file placement for the frequently used applications. In Windows 2000/XP, these options are called Drive Options.

If you change any Drive Options or Global Options settings, including the maximum number of disks to optimize concurrently, you must restart Speed Disk before the changes take effect.

To set Speed Disk options in Windows 2000/XP

1. In the Speed Disk main window, click **Drive Options**.
2. Click a tab to customize Speed Disk options.

To set Speed Disk options in Windows 98/Me

1. In the Speed Disk main window, click **Properties**.
2. Click **Options**.
3. Click **Customize**.
4. Click a tab to customize Speed Disk options.

   See "Use online Help" on page 93.

   For more information on these settings, see the online Help.
5. Click **OK**.

Specify file placement during optimization

In general, Speed Disk default settings for placing files provide the best performance. Change the disk's default settings only if your files require special consideration. For example, if you use a disk utility that updates certain file dates even when those files have not been used, you may want to limit optimization on these files so that Speed Disk doesn't move them to the area of the disk that is reserved for frequently used files.

If you want to place files in a specific location, which overrides the Speed Disk default file placement, use the Drive Options view. This view lets you select files or *file types* and specify where they should be placed during optimization.

See "Use online Help" on page 93.

For more information about Speed Disk optimization capabilities and customization, see the online Help.

Schedule optimization

In Windows 2000/XP, in addition to scheduling times for disk optimization, Speed Disk Schedule Options let you select a fragmentation threshold. When the selected disk reaches the specified degree of fragmentation, Speed Disk automatically optimizes it. You can select Auto Threshold or enter a percentage. The default fragmentation percentage threshold is determined by the disk's fragmentation level and is managed by the Auto Threshold feature.

For example, if you set the fragmentation threshold to 5% (within the recommended range), Speed Disk begins optimizing in the background when the level reaches 5%.

The threshold setting only applies to disk optimizations that you schedule. The schedule must be enabled for this setting to take effect.

To set an optimization schedule by threshold in Windows 2000/XP

1. In the Speed Disk main window, in the Select a View pane, click **Schedule Options**.
2. Check **Enable Schedule**.
3. Check **Optimize Based On Threshold**.
   Auto Threshold is enabled by default, which causes Speed Disk to optimize the selected disk when fragmentation goes over an amount that is determined by the disk characteristics.
4. To specify another threshold, check **Only Optimize Drive If Fragmentation Exceeds**:, then type a percentage value.
   The recommended percentage is between 2% and 5%. This ensures that Speed Disk optimizes the disk when the fragmentation percentage reaches the level that you specify at the scheduled time.
5. Click **Apply**.

Optimize registry and swap files

Windows creates a special file on your disk called a swap file (also called a paging file). This file is used to create additional memory so that your Windows programs can make maximum use of available system resources. The size of the file changes dynamically in response to demand for memory space. This can cause significant fragmentation of the file, which in turn reduces performance.

Another Windows component that can affect system performance is the Windows registry. The registry is a dynamic database of configuration settings for the operating system and applications. Over time, the internal structure of this database can become disordered. This disorder can also affect system performance.

About the Windows swap file

The swap file is vital to Windows performance. Windows uses this file for temporary data storage, which frees up more of the faster physical memory (RAM) for applications. The swap file grows and shrinks dynamically to meet changing system conditions.

Because the swap file changes continuously, it can become fragmented quickly. When the swap file is fragmented, Windows performance suffers. By default, Speed Disk defragments and optimizes the swap file to help maintain optimal Windows performance.

If the swap file is located in the midst of other changing files on the disk, its high rate of fragmentation can result in the other files becoming more fragmented than they otherwise would. To minimize the fragmentation that can result from frequent swap file changes, Speed Disk normally places the swap file last on the disk, after the other files and before the consolidated free space. This speeds future optimizations.

Specifying a minimum size for the swap file causes Windows to reserve space on the disk for it. This can keep the size of the swap file relatively stable. If you have specified a minimum size for the swap file, Speed Disk places it first on the disk for optimal Windows and application performance.

About the Windows registry

The registry is a large database used by Windows and other applications to store hardware and software configuration information. Information is continually written to and deleted from the registry during the course of everyday computer use.

When data is deleted from the registry, the space that was occupied by the data is not always immediately reused. Such leftover space in the registry can prevent data from being stored efficiently, and can cause the registry to take up more space in memory and on disk than is absolutely necessary.

Optimize the registry and swap file in Windows 98/Me

Norton Optimization Wizard sets a minimum swap file size to reduce file fragmentation, and reorganizes the Windows registry data for efficient storage and retrieval.

Close all programs before you run Norton Optimization Wizard. If a program attempts to alter the registry while Norton Optimization Wizard is optimizing it, the settings that it is attempting to save are lost. Also, do not empty the Recycle Bin or change Windows settings during registry optimization.

To optimize your registry and swap file in Windows 98/Me

1. On the left side of the main window, click **Norton Utilities** > **Optimize Performance**.
2. Click **Norton Optimization Wizard**.
3. Click **Next**.
   Norton Optimization Wizard checks your swap file and ensures that it is on the fastest available disk.
4. In the Optimize your Swap File pane, check **Configure Swap File for optimal performance**, then click **Next**.
   Norton Optimization Wizard offers to optimize your registry.
5. Check **Optimize my Registry**, then click **Next**.
   Norton Optimization Wizard summarizes the choices that you have made and warns you that you must restart your computer to complete the optimization process.
6. Close any other programs that are running, then click **Reboot**.
   Norton Optimization Wizard implements your choices and restarts your computer.

Run Speed Disk from the command line

You can run Speed Disk from the command line, from a console window, or a DOS window, or by clicking Run on the Start menu and typing a command using the command-line syntax. Whatever options you use when you run Speed Disk from the command line override any other options that you previously selected while running Speed Disk in any version of Windows.

Windows 98/Me command-line syntax

For Windows 98/Me, use the following syntax:

SD32 [drive:]...[/F | /U | /Q]

The following options can be entered in any order:

drive	Optimizes the specified drives. Each drive letter that is specified must be followed by a colon. This option overrides any that were previously selected in Speed Disk.
/F	Full optimization.
/U	Defragment files only.
/Q	Quick defragmentation of free space only.

For example, to start Speed Disk from the command line so that it performs a quick optimization of drive E, you type:

SD32 E: /Q

Windows 2000/XP command-line syntax

For Windows 2000/XP, use the following syntax:

```
sdntc -drive=<drive letter>:
```

The following options can be entered in any order:

-drive	Specifies the drives to be optimized.
-auto	Causes Speed Disk to start optimizing.

For example, to start Speed Disk from the command line and automatically optimize drive C, you would type:

```
sdntc -drive=c: -auto
```

Eliminating data permanently

15

Wipe Info lets you remove selected files or folders from your hard disk. You can also wipe free space from your hard disk, ensuring that previously deleted sensitive information is not left behind.

If you are running a recovery application such as System Restore or Norton GoBack, you must erase your history before running Wipe Info to ensure that the data is completely wiped.

About Wipe Info

Wipe Info erases files or folders from your hard disk so that they cannot be recovered. Wipe Info can also wipe the free space on your hard disk.

When you wipe a file, Wipe Info wipes the file and attempts to wipe any free space that is associated with the file and the file’s directory entry.

When you wipe a folder, Wipe Info wipes all of the files in the folder, and then, if the folder is empty, it attempts to wipe the directory entry for the folder.

When you wipe free space, Wipe Info wipes the free drive space, free file space, and erased file entries.

In general, you cannot recover files that have been wiped. Windows Me/XP System Restore can restore files that have been wiped if they are one of the protected file types. By default, many document types, such as .doc and .xls files in My Documents, are protected. Windows Me/

XP System Restore maintains copies of protected files. Wiping the original file does not wipe the copy that Windows Me/XP System Restore maintains.

Wipe Info eliminates a file's contents from the disk, but does not remove the file name. While the file name remains on disk, it is no longer visible in Windows Explorer, and there is no data stored with it. On NTFS volumes, streams (alternate data that belongs to a file but is not stored with the file) are also wiped.

Never store sensitive information in a file name or attribute. This data can be replicated throughout your system without your knowledge, for example, in a list of most recently used files, or a file name search. This type of embedded information can be very difficult to remove from your computer.

About hexadecimal values

Wipe Info uses hexadecimal values to wipe files. Hexadecimal refers to the base 16 number system. This system is used by computer programmers to represent numbers in the binary number system, which uses the zero and one symbols in combinations to represent any number.

The hexadecimal system consists of the numbers 0 to 9 and the letters A to F, used in combinations. For example, the decimal number 14 is represented as the letter E, as in 0Eh in the hexadecimal system.

In Wipe Info options, you can specify values from 00 to FF, representing numbers from 0 to 255 respectively. You can type the value using a number or a character from A to F.

About the Government Wipe process

When you select Government Wipe, Wipe Info does the following:

- Overwrites the data with 00s
- Verifies the 00 overwrite
- Overwrites with FFs

- Verifies the FF overwrite
- Writes a random value, or a value that you choose from 00 to FF
- Verifies the random overwrite
- Reverifies the random overwrite to ensure that it was written correctly
- Repeats as many times as you specify, up to 100

Set Wipe Info options

You can specify how Wipe Info handles *hidden*, read-only, and system files. You can also specify the type of wipe to use. The following wiping methods are available:

Fast Wipe	Overwrites the data that is being wiped with the hexadecimal value of your choice
Government Wipe	Combines several wiping and overwriting processes to conform to specifications in DoD (United States Department of Defense) document 5220-22-M, National Industrial Security Program Operating Manual, for the ultimate security level when eliminating data from digital media See "About the Government Wipe process" on page 248.

To change Wipe Info options in Windows 2000/XP

1 On the left side of the main window, click **Norton Utilities** > **System Maintenance** > **Wipe Info**.

2 In the Wipe Info window, on the View menu, click **Options**.

3 On the General tab, select the options for Read-only, System, and Hidden file types.

4 On the Wipe Type tab, select one of the following:

- Fast Wipe
- Government Wipe

See "About hexadecimal values" on page 248.

5 In the Hex Value text box, type the hexadecimal values that Wipe Info should use when it overwrites the wiped files space.

6 In the Times to Perform This Wipe text box, type the number of times that Wipe Info should repeat this process.

7 Click **Apply**.

To change Wipe Info options in Windows 98/Me

1 On the Options menu, click **Norton Utilities** > **Wipe Info Settings**.

2 On the Wipe Info Settings tab, specify the settings that you want. Your options are:

Display Wipe Info icon on the desktop	Create a Wipe Info shortcut on the Windows desktop. You can drag items to this icon to wipe them.
Number of times to repeat the delete	Type the number of times that you want Wipe Info to repeat the wiping process.

3 Select a wipe type. Your options are:

Fast Wipe	Under Write once the value, specify the value that Wipe Info should use when it writes over the wiped file space. The value can be up to 9 digits, and the default is 0 (zero).
Government Wipe	Under Number of times to repeat this, specify the number of times that Wipe Info should repeat the process of writing all 1s and 0s, then type the value that Wipe Info should use for a final write. The final write is verified to ensure that no disk errors caused sensitive data to survive the wiping process.

4 Click **OK**.

Wipe files or folders

To wipe a file or folder in Windows 2000/XP, add it to the Wipe Info window.

To wipe files or folders in Windows 2000/XP

1. On the left side of the main window, click **Norton Utilities** > **System Maintenance** > **Wipe Info**.
2. In the Wipe Info window, click **Browse**.
3. Select one of the following:
   - Folders
   - Files
4. Select the folder or file to delete.
5. Click **Open**.
6. If you add an item to the list by mistake, select the item, then click **Remove Item(s) from list**.
7. Click **Wipe All**.
8. If a warning message appears, click **Yes** to confirm the deletion.
   All of the files in the list are wiped.

As a short cut, you can drag the selected item from your desktop to the open Wipe Info file list. Continue to drag all of the files and folders that you want to wipe into the Wipe Info list.

To wipe free space in Windows 2000/XP

1. On the left side of the main window, click **Norton Utilities** > **System Maintenance** > **Wipe Info**.
2. On the Actions menu, click **Wipe Free Space**.
3. In the Wipe Free Space dialog box, select a disk.
4. Click **Go**.

In Windows 98/Me, Wipe Info uses a wizard to automate the wiping process.

To wipe files or folders in Windows 98/Me

1 On the left side of the main window, click **Norton Utilities** > **System Maintenance** > **Wipe Info**.

2 In the Wipe Info Wizard, select Files, Folders, or Free Space, then click **Next**.
Depending on which item you select, your options might vary. Your options are:

Files	Wipe Info deletes the selected file, its directory entry if possible, and any associated free space.
Folders	You can specify whether subfolders should be included. Wipe Info deletes all files in the selected folder, its directory entry if possible, and any associated free space.
Free Space	Wipe Info wipes the free space on the selected disk. This includes free disk space, file slack space, and erased file entries that are not in the Recycle Bin. (You must empty the Recycle Bin to have deleted files wiped.) Wipe Info verifies the disk's integrity before wiping free space. If the disk has problems, you are prompted to run Norton Disk Doctor.

3 Select the file, folder, or disk, then click **Next**.

4 If you see a warning message, click **Yes** to proceed.

See "Set Wipe Info options" on page 249.

5 For Wipe Options, select one of the following:

- Fast Wipe
- Government Wipe

6 In the Wipe Summary window, review what Wipe Info will do, then click **Next**.

7 If you want to change any selections, click **Back**.
Wipe Info displays its progress and summarizes the results, including any problems that were encountered during the wiping process.

8 View the results, then click **Close**.

Viewing computer information

16

No matter what your level of computer expertise, difficult questions about your computer's configuration will arise. For example, when you have a problem installing new hardware or software and you call the manufacturer for technical support, you may be asked questions about your computer's BIOS, bus type, processor, ports, video and multimedia capabilities, or memory capacity. Having access to this information is useful.

Use System Information

System Information gives you quick and easy access to information about your computer. It provides technical details about the following:

- System configuration (processor, BIOS, bus type, memory, and more)
- Display (video *driver*)
- Printers and printer ports
- Physical and virtual memory
- Disk drives
- Input devices (keyboard and mouse or other pointing device)
- Multimedia devices
- *Network* connections

This information can be saved to your disk or printed.

To use System Information

1 On the left side of the main window, click **Norton Utilities** > **System Maintenance** > **System Information**.
System Information gathers information about your computer and displays it on tabs in the System Information dialog box. You can print the information on one tab or on the entire inventory.

2 Click each tab to view the information on that tab.

3 When you have finished viewing the information, click **Close**.

For network, CD, and compressed drives, the Disk Usage Selection on the Drive tab is the total size of all of the selected items as reported by the file system. This does not include space that is wasted due to the device's cluster size. The total amount that is allocated is often slightly more than the size that is displayed by System Information. These snapshots of your system are helpful when you call a vendor for technical support.

See "Use online Help" on page 93.

For more information, see the online Help.

4

Norton CleanSweep

Removing unwanted files and programs

17

When you use your computer, you sometimes install programs that remain on your hard disk after you no longer need them. It's also easy to accumulate files (for example, pictures and media files) that are used once and remain on your hard disk, which takes up space. Norton CleanSweep cleans unwanted files and programs from your hard disk.

Safety Sweep makes a backup copy as it removes programs and files so that you can restore the program or file later. Safety Sweep also works with Uninstall Wizard to identify programs and files that are safe to remove.

Enable and disable Safety Sweep

Enable Safety Sweep to protect important files and programs from accidental removal. Disable Safety Sweep when you want to delete previously protected files and programs.

To enable or disable Safety Sweep

1 On the Options menu, click **Norton CleanSweep**.

2 On the Safety Sweep tab, in the Safety Sweep group, select one of the following:

- On
- Off

3 Click **OK**.

Identify files that are safe to remove

Safety Sweep provides the following indicators that tell you how safe it is to remove various files:

Green indicator	The file is safe to remove. When Safety Sweep is on, Norton CleanSweep lets you remove files with green indicators.
Yellow indicator	The file should be deleted with caution.
Red indicator	The file is in use or protected and cannot be removed. You cannot change the status of a file that is marked red. See "I can't delete files that Norton CleanSweep has marked red" on page 323.

Use Fast & Safe Cleanup

See "Set Fast & Safe Cleanup options" on page 118.

Norton CleanSweep Fast & Safe Cleanup finds and deletes specific file types that are safe to remove, such as temporary files, Internet browser cache files, and files in the Windows Recycle Bin. You can use Fast & Safe Cleanup any time to free hard disk space instantly, and on a regular schedule to keep your disk free of clutter.

If you are connected to the Internet, close your browser before you run Fast & Safe Cleanup.

To use Fast & Safe Cleanup

1. On the left side of the main window, click **Norton CleanSweep** > **CleanUp**.
2. Click **Fast & Safe Cleanup**.
   Fast & Safe Cleanup scans your hard disks and displays an estimate of how much disk space can be reclaimed by deleting unnecessary files.
3. Click **Clean Now**.
4. In the Space Freed dialog box, click **OK**.

Remove unwanted programs

Norton CleanSweep lets you remove unwanted programs to free disk space. Uninstall Wizard deletes not only a program's individual files, but also any external references to the files, such as program icons or entries in system configuration files. Uninstall Wizard creates a backup of the program that it keeps for as long as you specify. You can use Restore Wizard to restore these backed-up programs.

See "Backing up and restoring programs" on page 273.

If you need to restore the program, Backup Wizard creates a single, compressed backup file for use as a reserve, which leaves all of the original files and configuration information in place.

You can also use the Windows shortcut menu on the desktop or in Windows Explorer to select a program for Norton CleanSweep to remove.

Do not use Norton CleanSweep to remove Norton SystemWorks. Instead, use Add/Remove Programs in the Windows Control Panel. See "If you need to uninstall Norton SystemWorks" on page 60.

Remove a program with Uninstall Wizard

Uninstall Wizard displays a program tree that you can use to identify the program that you want to remove. The program tree includes the following expandable folders:

Start Menu	Programs on the Start menu
Desktop	Any shortcut icons on the desktop

Programs Monitored By Smart Sweep	Any programs that have been monitored by Smart Sweep (if you have not yet monitored any program installations, the folder is empty and the folder's description is No Programs Monitored By Smart Sweep)
Downloads Monitored By Internet Sweep	Any ActiveX controls that have been monitored by Internet Sweep (if you have not yet monitored any ActiveX control installations, the folder is empty and the folder's description is No Downloads Monitored By Internet Sweep)

To uninstall a program with Uninstall Wizard

1. On the left side of the main window, click **Norton CleanSweep** > **CleanUp**.
2. Click **Uninstall Wizard**.
3. Select the program to remove, then click **Next**.
4. Follow the on-screen instructions to proceed.
5. Specify whether or not you want to back up the selected program and confirm the deletion of each item in the program. Your options are:

Finish	Remove the entire program.
View	View, add to, or remove from the list of components that will be uninstalled. See "Remove part of a program" on page 261 and "View more information about a component" on page 262.

6. Click **OK** to confirm the program removal.
   A dialog box reports the action as completed and asks if you want to see a summary that contains a detailed description of the actions that were performed.

During an uninstallation, Uninstall Wizard might disappear behind other open windows on your computer. However, Uninstall Wizard reappears once the uninstallation is complete.

To uninstall a program using the shortcut menu

1 In Windows Explorer, right-click the application to remove, then click **CleanSweep** > **Uninstall Wizard**.

2 Follow the on-screen instructions to proceed.

3 Specify whether or not you want to back up the selected program and confirm the deletion of each item in the program. Your options are:

Finish	Remove the entire program.
View	View, add to, or remove from the list of components that will be uninstalled. See "Remove part of a program" on page 261 and "View more information about a component" on page 262.

4 Click **OK** to confirm the program removal.
A dialog box reports the action as completed and asks if you want to see a summary that contains a detailed description of the actions that were performed.

During an uninstallation, Uninstall Wizard might disappear behind other open windows on your computer. However, Uninstall Wizard reappears once the uninstallation is complete.

Remove part of a program

You can remove components of a program rather than the entire program with Uninstall Wizard. For example, if a component is shared with another program or if it contains data that you want, you might want to keep it.

To remove part of a program

1 On the left side of the main window, click **Norton CleanSweep** > **CleanUp**.

2 Click **Uninstall Wizard**.

3 In Uninstall Wizard, click **View**.
The components of the program to be removed are checked.

4. To prevent a component from being uninstalled, uncheck it.
5. Click **OK**.

View more information about a component

In the Program Selection dialog box, you can perform various actions with a program component before you remove it.

Component type	**Action**
Text file	View the file contents.
Program file	View the Windows system information.
Executable program	Start the program using the Run button.
Executable program Dynamic Link Library (DLL) file or Visual Basic extension file	See a description of any DLL files that the program uses or any programs that depend on the file using the Link button.

To view more information about a component

1. On the left side of the main window, click **Norton CleanSweep** > **CleanUp**.
2. Click **Uninstall Wizard**.
3. In Uninstall Wizard, click **View**.
   The components that are selected for removal are checked.
4. Select a component to view, then click **View**.
5. When you have finished viewing the component information, click **OK**.

If you want to add a component to uninstall

You can add components to be uninstalled. Components include files and selected sections of the WIN.INI file. You can select one component at a time.

To add a component to uninstall

1. In Windows Explorer, right-click the application to remove, then click **CleanSweep** > **Uninstall Wizard**.
2. Follow the on-screen instructions to proceed.
3. In the Add Component dialog box, do one of the following:
   - Click **File**, then select a file.
   - Click **WIN.INI Section**, then select a section of your computer's WIN.INI file in the list.
4. To view the contents of your selected component, click **View**.
5. Click **OK**.

If you want to display program links

You can view the links to a program that you want to uninstall. Links are files that do one of the following:

- Use or rely on the selected component.
- Are files that the selected components uses or relies on.

This information might help you to decide if you want to modify the component that you want to uninstall.

To display program links

1. On the left side of the main window, click **Norton CleanSweep** > **CleanUp**.
2. Click **Uninstall Wizard**.
3. Start the uninstallation of a program with Uninstall Wizard.
   See "Remove a program with Uninstall Wizard" on page 259.
4. In Uninstall Wizard, click **View**.
   The components that are selected for removal are checked.
5. Select a component to view, then click **Links**.

6 In the Links dialog box, select the type of links that you want to view. Your options are:

List files that use this file	Displays a list of all the files in the program group that use the selected file
List files that this files uses	Displays a list of files that the selected file depends on

7 Click **OK**.

Use summary information

See “Use the Norton CleanSweep Master Log” on page 117.

When Uninstall Wizard is finished, a Summary dialog box displays the completed activity. This activity is also recorded in the Master Log.

The summary includes the following:

- Date and time the uninstallation was performed
- Name of the component that was uninstalled
- Backup destination, if applicable
- Description of the program
- Number of bytes that were deleted

Removing Internet clutter

When you visit a Web site, you accumulate temporary *cache* files, *cookies*, browser plug-ins, and *ActiveX* controls. Many of these files are used once but they remain on your hard disk until you remove them.

Uninstall programs and remove files

Norton CleanSweep uses the following features to uninstall programs and remove files that were *downloaded* from the Internet:

Internet Uninstall	Uninstalls programs that were downloaded from the Internet. See "Uninstall programs that were downloaded from the Internet" on page 266.
Internet Cache Cleanup	Removes temporary files that are stored by Web browsers. See "Remove Internet cache files" on page 267.
Cookie Cleanup	Removes Internet cookie files. See "Manage cookies on your computer" on page 267.
Plug-in Cleanup	Removes Web browser plug-ins. See "Remove unwanted plug-ins" on page 269.
ActiveX Cleanup	Removes ActiveX controls that were downloaded from the Internet. See "Remove unwanted ActiveX controls" on page 270.

The Norton Cleanup Internet features are available if you have the following:

- A connection to the Internet
- An Internet service provider (*ISP*)
- Microsoft Internet Explorer 5.5 or later, or Netscape Navigator 4.7 or later
- America Online users must use AOL Internet Explorer OEM version 5.0 or later

Uninstall programs that were downloaded from the Internet

When you browse the Internet, you sometimes *download* programs that you use temporarily or that become obsolete. These programs remain on your hard disk, and take up space. Internet Uninstall removes these programs from your hard disk.

To uninstall a program

1. On the left side of the main window, click **Norton CleanSweep** > **Internet**.
2. Click **Internet Uninstall**.
   Uninstall Wizard displays a program tree that lists installations that were monitored by Internet Sweep.
3. Select the program to remove, then click **Next**.
4. Follow the on-screen instructions to proceed.
5. Specify whether or not you want to back up the selected program and confirm the deletion of each item in the program. Your options are:

Finish	Remove the entire program.
View	View or modify the list of components that will be removed.

6. Click **OK** to confirm the program removal.
   A dialog box reports the action as completed and asks if you want to see a summary that contains a detailed description of the actions that were performed.

Remove Internet cache files

Internet *cache* files are temporary files that are used by your Internet browser to store copies of each Web page that you visit. A browser can display the page more quickly by retrieving it from the cache than by retransmitting it from the Web site. Internet Cache Cleanup frees valuable disk space. Remove your Internet cache files frequently if you use the Internet and online services often. The deleted cache information reloads automatically from the Web.

Before you remove cached files, close your Internet browser if it is open.

To remove Internet cache files

1. On the left side of the main window, click **Norton CleanSweep** > **Internet**.
2. Click **Internet Cache Cleanup**.
   Internet Cache Cleanup scans your disk for Internet cache files and displays an estimate of the disk space that is currently occupied by Internet cache files.
3. In the Internet Cache Cleanup dialog box, click **Clean**.
   A message informs you that the Internet cache files will not be backed up.
4. Click **Yes** to respond to the message.
   Internet Cache Cleanup displays a summary of files that will be deleted.
5. To view a log of the activity, click **View**.
6. Click **Finish**.
   Internet Cache Cleanup deletes the Internet cache files, and displays a message when it is finished.
7. Click **OK**.

Manage cookies on your computer

Cookies are small data files that are placed on your hard disk while you are browsing the Internet. Web sites that you visit use small programs to place cookies on your hard disk so that they can track your preferences and browsing habits.

Decide which cookies to keep

All *cookies* are safe to remove; you do not need to back them up. However, if a cookie came from a Web site where you make purchases or conduct business or confidential transactions, it might contain a password or code for verification of your identity. If you remove this type of cookie, you might have to enter personal information on the Web site again.

If you revisit a Web site whose cookie you removed, it creates a new cookie.

To view a cookie's information

1. On the left side of the main window, click **Norton CleanSweep** > **Internet**.
2. Click **Cookie Cleanup**.
3. Select a cookie whose information you want to view.
4. Click **View**.

Remove unwanted cookies

Before you can use Cookie Cleanup, you must disable Safety Sweep.

See "Enable and disable Safety Sweep" on page 257.

To remove unwanted cookies

1. On the left side of the main window, click **Norton CleanSweep** > **Internet**.
2. Click **Cookie Cleanup**.
3. Do one of the following:
   - To remove all cookies, click **Select All**.
     If cookies are marked yellow or red, Cookie Cleanup does not let you remove them.
   - To remove specific cookies, check the cookies that you want to remove.
4. Click **Clean**.
5. In Cookie Cleanup Wizard, follow the on-screen instructions to remove the cookies.
   It's safe to remove cookies without making backups.
6. In the Cookie Cleanup dialog box, click **Close**.

See "Decide which cookies to keep" on page 268.

Remove unwanted plug-ins

Plug-ins enhance Web browsing by letting you view certain document types, watch video, or listen to live or recorded audio.

Plug-ins can take up significant hard disk space, so if you do not use a plug-in regularly, you can remove it. Plug-ins are safe to remove. You can back them up if you plan to use them again.

See "Uninstall programs that were downloaded from the Internet" on page 266.

Use Plug-in Cleanup if Smart Sweep did not monitor the installation. If Smart Sweep did monitor the installation, use Internet Uninstall to remove the plug-ins.

Before you remove plug-ins, close your Internet browser if it is open.

To remove unwanted plug-ins

1 On the left side of the main window, click **Norton CleanSweep** > **Internet**.

2 Click **Plug-in Cleanup**.

3 Do one of the following:
   - To remove all plug-ins, click **Select All**.
   - To remove specific plug-ins, check the plug-ins that you want to remove.

   If Safety Sweep is on, you must turn it off to select a file that is color-coded yellow. While a file is selected, click **Advise** to see more information about the file and advice on what to do with it, or click **View** to view the file.

4 Click **Clean**.

5 In Plug-in Cleanup Wizard, follow the on-screen instructions to remove the plug-ins.

6 In the Plug-in Cleanup dialog box, click **Close**.

Remove unwanted ActiveX controls

ActiveX controls enhance Web pages with interactive content. They activate when you visit a Web page that contains ActiveX content. The first time that a page is visited, its ActiveX controls are *downloaded* to your hard disk. Internet Sweep monitors ActiveX controls and their locations.

All ActiveX controls are safe to remove; you do not need to back them up. If you revisit a Web site whose ActiveX control you removed, it downloads the ActiveX control again.

Norton CleanSweep does not let you remove the ActiveX controls that are used by Windows 98. It lets you view and remove only those ActiveX controls that are downloaded from the Internet.

See "Uninstall programs that were downloaded from the Internet" on page 266.

Use ActiveX Cleanup if Internet Sweep did not monitor the installation. If Internet Sweep did monitor the installation, use Internet Uninstall to remove the ActiveX controls.

Before you remove ActiveX controls, close your Internet browser if it is open.

To remove ActiveX controls

1. On the left side of the main window, click **Norton CleanSweep** > **Internet**.
2. Click **ActiveX Cleanup**.
3. In the ActiveX Control Cleanup dialog box, do one of the following:
   - To remove all ActiveX controls, click **Select All**.
   - To remove specific ActiveX controls, check the ActiveX controls that you want to remove.
4. Click **Clean**.
5. In ActiveX Control Cleanup Wizard, follow the on-screen instructions to remove the ActiveX controls. When the cleanup is complete, ActiveX Control Cleanup Wizard displays a summary.
6. Click **Finish**.
7. To close the ActiveX Control Cleanup dialog box, click **Close**.

Backing up and restoring programs

19

Norton CleanSweep Backup Wizard safely compresses infrequently used programs to provide more disk space. You can move the compressed backup to a new location or copy it to a different computer. Restore Wizard ensures that all of the program's related files are restored when you want to use the program again. It also restores registry values.

Back up programs

Backup Wizard creates a single, compressed backup of a program for use as a reserve in the event that you need to restore the program.

To back up a program

1. On the left side of the main window, click **Norton CleanSweep** > **Programs**.
2. Click **Backup Wizard**.
3. In the Backup Wizard program list, select the file or program to back up.
   Backup Wizard analyzes the program.
4. Verify the backup folder location, then click **Next**.
   Backup Wizard displays a summary of the files that will be backed up.
5. To confirm the actions that will be taken by Backup Wizard, click **Finish**.
6. When Backup Wizard has finished, click **OK**.

Delete unwanted backups

Norton CleanSweep maintains compressed backup files of uninstalled programs. Once you are sure that you no longer want to restore a program, you can delete its backup.

To delete a backup

1. On the left side of the main window, click **Norton CleanSweep** > **Programs**.
2. Click **Restore Wizard**.
   Restore Wizard displays a list of backed up programs.
3. Select the backup to delete, then click **Delete**.
   Backup Wizard displays a summary of what will be deleted.
4. Click **Yes** to delete the backup.
   The backup is deleted, and no longer appears in the list of backed up programs.
5. Click **Cancel** to return to the main window.

Delete a backup in response to an alert

Norton CleanSweep alerts you to keep an existing backup or delete it to make more hard disk space available.

To delete a backup in response to an alert

1. In the Old Backup Files alert, click **Yes**.
2. In Restore Wizard, ensure that the item you want to delete is selected.
3. Click **Delete**.
4. Click **Yes** to confirm the deletion.

Restore a backed up program

Restore Wizard uses a Norton CleanSweep backup to restore a program to its original state.

To restore a backed up program

1. On the left side of the main window, click **Norton CleanSweep** > **Programs**.
2. Click **Restore Wizard**.
3. Select the backup to restore, then click **Next**.
4. In the selected backup, select the items that you want to restore. Your options are:

All the files	Restore all of the files that are associated with the program.
Only the files selected below	Specify the files to restore before you proceed.

5. Click **Next**.
6. Specify how you want Norton CleanSweep to proceed if a file that is being restored already exists, then click **Next**.
7. Click **Next** to accept the default setting and have Norton CleanSweep restore the files to the location where they were previously stored.
   You can also restore the files to a different location.
8. Click **Finish** to restore the backup.
9. In the Restore Complete dialog box, click **Yes** to delete the backup.
10. Click **OK**.

See "Restore a program to a different program group" on page 275.

Restore a program to a different program group

You can restore a backed-up program to a different location.

Some programs may malfunction if they are not restored to their original locations.

To restore a backed up program to a different location

1. On the left side of the main window, click **Norton CleanSweep** > **Programs**.
2. Click **Restore Wizard**.
   Restore Wizard displays a list of backed up programs.

3 Select a program to restore, then click **Next**.
Restore Wizard displays the original installed location.

4 Click **No, let me select the location**, then click **Next**.

5 Select or type a folder name for the restored program's new location.

6 Select the program group to which the program will be restored, then click **Next**.

7 Confirm the location to which the program will be restored.

8 To view a summary of what will be restored, click **View**.

9 Click **Finish**.
The program is restored to the selected program group location.

10 In the Restore Complete dialog box, specify what you would like to do with the backup files, now that the program has been restored. Your options are:

Yes	Delete the backup (recommended).
No	Keep the backup.

11 Click **OK**.

5

Norton SystemWorks Professional tools

Copying and cloning disk images

20

Norton Ghost creates clones, or exact disk images, of your hard disks. You can use these disk images in an emergency to restore a damaged disk, or to migrate the contents of your hard disk, complete with settings, to another computer.

Protect your computer with backups

Making backups of the data on your computer is an essential part of maintaining your computer. If you do not make regular backups, you risk losing all of the data if your hardware or software fails.

Once you have performed a backup, any changes made to your computer, or data that is created, are not included in the backup. If you enter data that is crucial to you, then you must back up those data files to ensure that you have a comprehensive disaster backup solution.

There are many ways you can back up the files on your computer. Norton Ghost backs up and restores entire images of your disks.

When to back up your computer

You should perform a backup of your system on a regular basis, for example, once a week, and keep more than just the most recent backup. If disaster occurs, you will lose no more than a week’s changes.

You should also perform a series of backups if you make major changes to your computer, for example, if you install a new operating system or new software. When making a major change, do the following:

- Back up your computer to capture the existing operating system and files.
- Make the change to your computer, for example, install the new operating system.
- Back up your computer to capture the changes again.

About restoring and recovering data

Restoring and recovering have different meanings when referring to computer files and data.

See "If a file is deleted or missing" on page 18.

When a file or data is damaged or lost, first try to recover the damaged or lost information using tools such as Norton Disk Doctor or UnErase Wizard. These tools repair or undo the damage that was done to a file or data. It is always best to try to recover, rather than restore, a damaged file.

If you are unable to recover the file or data, you can restore an undamaged copy. Restoring a file replaces a damaged file with a copy that was made before it was damaged. Restoring a file returns it to the state it was in when you made the backup. Any changes that you made after the date of the backup are lost when you restore a file.

Tools such as Norton Ghost, Image, or Norton GoBack can be used to restore a file if recovery fails.

Norton Ghost includes both Windows and DOS tools. You can use the Windows tools for most backup and recovery tasks. Use the DOS tools if you have a hard disk failure or cannot start Windows.

How Norton Ghost works

The basis of Norton Ghost is a cloning function that creates an image file that contains all of the information that is required to recreate a complete disk or partition. Image files contain a backup copy of an entire drive or one or more partitions. The image file can be restored to one or more partitions or disks, which replaces existing data.

Virtual Partition

The Virtual Partition is a partition that is created when you perform a backup, restore, clone, or other operation from Windows. All of the files that are required for the backup, restore, or clone are automatically installed into the Virtual Partition and the task is performed. Most of the Virtual Partition operation is not apparent to you, however, there may be some occasions when you must know what the Virtual Partition is and what it does, such as if you want to run Ghost.exe or another application from the Virtual Partition.

One primary partition slot must be available in the MBR for the Virtual Partition.

Hardware restrictions

Norton Ghost is designed to restore to and clone identical hardware. When Microsoft Windows is installed, drivers that are necessary to support your hardware are installed to the hard disk and recorded in the Windows operating system files. If you move an installation of Windows to another computer, either by directly moving the hard disk or copying it using a Norton Ghost operation, there is no guarantee that it will start or function correctly. Although Microsoft provides tools, such as Sysprep, that may alleviate these problems to volume license holders, these tools are usually unavailable to consumer or small business users.

A computer with Windows installed should be copied to a computer with identical hardware. Moving or cloning file systems that do not contain operating systems is not usually a problem.

Prepare for an emergency

See "Create and test a Ghost boot disk" on page 285.

After you have installed Norton Ghost and created a backup image, you must create and test a recovery boot disk in case of an emergency. If you experience a critical failure and cannot start your computer, then you must have a recovery boot disk. This lets you start your computer in DOS and run Norton Ghost to restore your computer.

If you saved your image file directly to CD or DVD, then you do not need a recovery boot disk. Norton Ghost includes Ghost.exe if you save the image file to CD or DVD.

There are two methods of restoring your computer:

Norton Ghost	If you are able to start in Windows, then you may be able to run Norton Ghost from Windows on your hard disk and restore your computer with the latest backup image file that you have created. See "Restore your computer from an image file" on page 289.
Ghost.exe	If you cannot start Windows, then you must start your computer from a recovery boot disk or CD/DVD. This starts your computer and starts Norton Ghost in DOS. In Norton Ghost you can access your image file and restore your computer to the latest backup image file. See "To restore your computer from an image file if you cannot run Windows" on page 291. The Ghost Boot Wizard helps you create a recovery boot disk. You should create and test a recovery boot disk before you need it. If your computer crashes and you do not have a recovery boot disk, then you will have to find another computer on which to create a boot disk. See "Create and test a Ghost boot disk" on page 285.

Norton Ghost components

Norton Ghost includes the following programs and utilities:

Norton Ghost Wizards	Norton Ghost includes Windows wizards to guide you through the basic tasks. These wizards include the following: ■ Backup Wizard: Lets you select a hard disk or partition to back up to an image file. ■ Restore Wizard: Lets you restore a hard disk or partition from an image file. ■ Clone Wizard: Lets you clone a hard disk or partition directly from another hard disk or partition. ■ Peer-to-Peer Wizard: Starts Ghost.exe in the Virtual Partition with the peer-to-peer drivers loaded. ■ Create Virtual Partition Wizard: Restarts your computer in the Virtual Partition in DOS with files from a selected directory. This enables you to run DOS applications. ■ Run Ghost Interactively Wizard: Restarts your computer in DOS and runs Ghost.exe. ■ Ghost Boot Wizard: Creates boot disks that start Norton Ghost when you turn on your computer. You can create boot disks for various cloning tasks. The wizard guides you through adding the drivers that are needed to create a boot disk.
Integrity Check	The image Integrity Check runs an Integrity Check on backup image files.
View Log	You can view logs that were created during Norton Ghost operations.
Norton Ghost executable (Ghost.exe)	Ghost.exe runs in DOS and lets you back up, restore, and clone your computer. Because the executable is small and has minimal conventional memory requirements, you can run it from a DOS boot disk or hard drive.

Ghost Explorer	Ghost Explorer is a Windows application that lets you view directories and files in an image file. You can also add, recover, and delete individual directories and files from a FAT16/32 file system image file. ⚠ You can restore individual files from NTFS images, but you cannot update NTFS images.
GDisk	GDisk is a complete replacement for the Microsoft FDISK and FORMAT utilities that lets you do the following: ■ FAT file system formatting ■ Batch mode operation ■ Hide and unhide partitions ■ Secure disk wiping to United States Department of Defense standards ■ Extensive partition reporting ■ Boot.ini manipulation (GDisk32 only) Two versions of GDisk are supplied: ■ GDisk: Runs in DOS ■ GDisk32: Runs from the command prompt in Windows
Ghost Walker	Ghost Walker assigns a statistically unique security identifier (SID) and a unique computer name to cloned Microsoft Windows NT/2000/XP computers. The SID is an important part of the Windows NT/2000/XP security architecture as it provides a unique identifier when these computers are networked. If you are cloning more than one computer using the multiuser pack, you can use Ghost Walker to set up each computer on a network with a unique identification.

Create and test a Ghost boot disk

See "Create a backup image file" on page 287.

Creating a Ghost boot disk is a one-time activity. You can create disk image files separately. Creating backup image files should be done regularly. When you create a Ghost boot disk, you should immediately test it to ensure that it will start your computer.

You need a Ghost boot disk to restore your computer after a software or hardware failure, or to clone the hard disk of a computer that does not have Windows installed. You do not need a Ghost boot disk to run the Backup, Restore, and Clone Wizards.

See "Access the User's Guide PDF" on page 94.

For more information, see the *Norton Ghost User's Guide* on the program CD.

Depending on the files that are included on the boot disk, you may require more than one blank floppy disk.

To create a Ghost boot disk

1. On the left side of the main window, click **Norton Ghost** > **Ghost Utilities** > **Norton Ghost Boot Wizard**.
2. In the Norton Ghost Boot Wizard, click **Standard Ghost Boot Disk**, then click **Next**.
3. In the Peer-to-Peer Options window, select the storage device support options that you want to install on the boot disk.
4. If you plan to save your image file to an external device, you may need to select one or more External Storage options. Your options are:

No USB Support	Add no support for USB devices to the boot disk.
USB 1.1 Support	Add support for USB 1.1 external devices to the boot disk.
USB 2.0 Support	Add support for USB 2.0 external devices to the boot disk.

Firewire Support	Add support for FireWire external devices to the boot disk.
Assign DOS drive letters	If you select an external storage option, Norton Ghost assigns a DOS drive letter to it.

5 Click **Next**.

6 In the DOS version window, click **Next**.

7 In the Ghost executable location window, verify the location, then click **Next**.

8 In the Destination Drive window, in the Floppy Disk Drive drop-down list, select the appropriate drive letter.

9 Ensure that Format disk(s) first is checked to format the disks before disk creation.

10 Ensure that Quick Format is checked to perform a quick format.

11 Click **Next**.

12 Review the boot disk details, then click **Next** to start creating the boot disks.

13 In the Format A:\ dialog box, click **Start** to format the floppy disk.

14 Click **OK** to confirm the formatting.

15 When the formatting is complete, click **OK**, then click **Close**.

You must test the Ghost boot disk or CD/DVD to ensure that you can run Ghost.exe and access your backup image file.

To test a Ghost boot disk

1 Do one of the following:

- Insert the Ghost boot disk into drive A and restart your computer.
- Insert the backup CD or DVD into the CD/DVD drive, restart your computer, then press any key to continue when you are prompted.
  Your computer restarts in DOS and launches Ghost.exe.

2. On the Ghost main menu, click **Local** > **Check** > **Image File**.
3. In the Disk Image file name dialog box, select the image file that you have created.
   To find the image file, next to File Image, click the down arrow. Select the drive on which you saved the image file to display the image file name.
4. Click **Yes** to proceed with the integrity check.
5. Once the integrity check is complete, click **Continue**.
6. Remove the Ghost boot disk or CD/DVD from the disk drive and restart your computer.

If the image passed the integrity check, you can restore your computer if Windows is not operational.

View an image file

You can check that your image file contains the files that you expect to see by opening and viewing it in Ghost Explorer.

To view an image file in Ghost Explorer

1. On the left side of the main window, click **Norton Ghost** > **Ghost Utilities** > **Norton Ghost Explorer**.
2. On the File menu, click **Open**.
3. Select the image file.
4. Click **Open**.

Create a backup image file

You can use Norton Ghost to create a backup image file of a disk or one or more partitions. When you create a backup image file, your computer is restarted in DOS for the image creation process. When the image has been created, your computer is restarted in Windows.

To create a backup image file

1. On the left side of the main window, click **Norton Ghost** > **Ghost Basic** > **Backup**.
2. Click **Next**.

3 In the Backup Wizard, in the Source pane, do one of the following:

- Select a disk to back up.
- Select one or more partitions to back up.
  The partitions must reside on the same disk.

4 Do one of the following:

- Click **File**, then click **Browse** to select a destination and file name to which the disk or partition is to be backed up.
- Click **Recordable CD or DVD** to back up to a CD or DVD drive.
  Norton Ghost selects the CD or DVD drive that contains writable media.

5 Click **Next**.

6 If this is the first time that you have used Norton Ghost on this computer, in the Add Ghost Disk Identification dialog box, click **OK** to identify all of the hard disks.
If you have previously used Norton Ghost on this computer, this dialog box does not appear.

7 In the Advanced settings window, click **Next**.

8 In the Important Information dialog box, click **Next**.
A dialog box warns you to check that you can run Ghost.exe and access your image file once it has been created.

9 In the Disaster Recovery window, click **Continue**.

10 In the Backup Wizard window, review the task details, then click **Run Now** to create the backup image file.
Your computer is restarted in DOS, the backup image file is created, and your computer is restarted in Windows.

Back up a hard disk or partition

If your image file is too large to fit on a CD or other *removable media*, Norton Ghost spans the image file onto multiple CDs and prompts you to insert another disk.

To back up a hard disk or partition

1. On the left side of the main window, click **Norton Ghost** > **Ghost Basic** > **Backup**.
2. Click **Next**.
3. In the Source list, do one of the following:
   - Select a disk to back up.
   - Select one or more partitions to back up.
4. Do one of the following:
   - Click **File**, then click **Browse** to select a destination and file name to which the disk or partition is to be backed up.
   - Click **Recordable CD or DVD** to back up to a CD or DVD drive.
     Norton Ghost selects the CD or DVD drive that contains writable media.
5. Click **Next**.
6. If this hard disk has not previously been fingerprinted, in the Add Ghost fingerprints dialog box, select a drive to fingerprint, then click **OK**.
   If you have previously used Norton Ghost on this computer, then this dialog box does not appear.
7. To set advanced driver settings for the backup, click **Driver Settings**.
   Norton Ghost automatically detects the required drivers. If this detection fails, then you may need to set the drivers in Driver Settings.
   For more information, see the *Norton Ghost User's Guide* PDF on the CD.

   See "Access the User's Guide PDF" on page 94.
8. Click **Run Now** to create the backup image file.
   Your computer is restarted and the backup image file is created.

Restore your computer from an image file

You can restore a hard disk or partition from an image file that is stored on another hard disk, partition, or external media in Windows.

If you cannot start Windows, you can use the Ghost boot disk to start your computer and restore your hard disk or partition.

Restore your computer only if you experience software or hard disk failure. The destination disk or partition is completely overwritten with no chance of recovering any data.

To restore your computer from an image file in Windows

1 On the left side of the main window, click **Norton Ghost** > **Ghost Basic > Restore**.

2 Click **Next**.

3 In the Select Image window, select a restore method. Your options are:

Restore from CD-R/ CD-RW	Restores the hard disk or partition from an image file that is stored on one or more CDs
Restore from a Norton Ghost Image File	Restores the hard disk or partition from a local image file

4 Click **Next**.

5 In the left pane, select the image file or partitions to restore.

6 In the right pane, select the destination hard disk or partitions that are to be overwritten.

7 Click **Next**.

8 If this is the first time that you have used Norton Ghost on this computer, in the Add Ghost fingerprints dialog box, select a drive to fingerprint, then click **OK**. If you have previously used Norton Ghost on this computer, then this dialog box does not appear.

See "Access the User's Guide PDF" on page 94.

9 To set advanced driver settings for the backup, click **Driver Settings**.
Norton Ghost automatically detects the required drivers. If this detection fails, then you may need to set the drivers in Driver Settings.

For more information, see the *Norton Ghost User's Guide* PDF on the CD.

10 Click **Next**.

11 Click **Restore Now** to restore the image file to the selected hard disk or partition.
Your computer is restarted and the restore operation is completed.

To restore your computer from an image file if you cannot run Windows

1 Do one of the following:
   - Insert the Ghost boot disk into drive A and restart your computer.
   - Insert the backup CD or DVD into the CD/DVD drive, restart your computer, then press any key to continue when you are prompted.
   Your computer restarts in DOS and launches Ghost.exe.

2 On the Ghost main menu, select a recovery method.
Your options are:

Local	Click **Local > Disk > From Image.**
Peer-to-peer connection	Click **Disk > From Image.**

3 In the File Locator dialog box, type the path and file name of the image file.

4 Select the drive or device.

5 Select the full path name.
The image file may reside on a local drive (but not the one to which it is being copied), or on a locally mapped network file server. If you are using peer-to-peer connections, the file is located on the destination computer.

6 Press **Enter**.

7 In the Destination Drive dialog box, select the destination disk.

Choose carefully as this is the disk that will be overwritten.

The Destination Drive dialog box shows the details of every drive that Norton Ghost finds on the local computer. If the source image file resides on a local disk, then this disk is not available for selection.

8 In the Destination Drive Details dialog box, confirm or change the destination disk partition layout.
The Destination Drive Details dialog box shows a suggested partition layout for the destination disk. By default, Norton Ghost tries to maintain the same size ratio between the new disk partitions. However, you should note the following:
   - You can change the size of any target FAT, NTFS, or Linux Ext2/3 partition by typing the new size in megabytes.
   - You cannot type a value that exceeds the available space, is beyond the file system's limitations, or is not large enough to contain the data that is held in the source partition.

9 Click **OK**.

10 Select one of the following:

Yes	Proceed with the disk cloning. Norton Ghost creates the destination disk using the source image file disk details. If you need to abort the process, press Ctrl+C, but be aware that this leaves the destination disk in an unknown state. ⚠ Only click Yes if you are sure that you want to proceed. The destination disk is completely overwritten with no chance of recovering any data.
No	Return to the menu.

11 If you are restoring from a spanned image, select one of the following:
   - OK: Continue on the same form of media.
   - Filename: Restore from a different location. Type the location and file name of the image file span.

12 When the disk image restore is complete, remove the second hard disk and restart your computer.

You should remove the second hard disk before you restart your computer. If you leave the second disk in the computer, damage can occur to both of the bootable operating systems.

Verify the integrity of a disk

Once you have performed a restore with Ghost.exe, verify the integrity of your disk.

To verify the integrity of a disk

1 On the left side of the main window, click **Norton Ghost** > **Ghost Advanced** > **Image Integrity Check**.

2 In the Image Integrity Check Wizard, click **Browse** to find the image file that you want to verify.

3 To view the contents of the image file in Ghost Explorer, click **Open Image in Ghost Explorer**.

4 Click **Next**.

5 To set advanced settings for the verification, click **Advanced Settings**.
For more information, see the *Norton Ghost User's Guide* on the CD.

6 Click **Next**.

7 In the Important Information dialog box, if you do not want to view this warning again, click **Don't show this screen again**, then click **Next**.

8 Click **Run Now** to start the image verification.

Access Norton Ghost information

The following information about Norton Ghost is available:

See "View Norton Ghost Help" on page 94.

- The Norton Ghost online Help is available on the Norton SystemWorks Help menu and in many Norton Ghost dialog boxes.

See "Access the User's Guide PDF" on page 94.

- The *Norton Ghost User's Guide* is available in PDF format on the CD.
- Tutorials are included on the CD to demonstrate common tasks.
- Links to selected knowledge base articles can be selected on the Help menu in the Ghost Boot Wizard, Norton Ghost, and Ghost Explorer.

The Symantec Ghost Web site (www.symantec.com/ghost) has answers to frequently asked questions, troubleshooting tips, online tutorials, a knowledge base, and the latest product information.

Benchmarking your computer

21

PerformanceTest is a software benchmarking tool that runs a series of tests and lets you assess the performance of your computer compared with other computers.

About PerformanceTest benchmarks

The PerformanceTest benchmarks measure the speed of your computer's CPU, math coprocessor, hard disk, CD/DVD-ROM drive, and other components. The tests also measure aspects of the graphics display.

Along with individual benchmarks, PerformanceTest includes a PassMark rating, a weighted average of test results that gives an overall indication of the computer's performance (the higher the number, the faster the computer).

You can let PerformanceTest run a standard series of tests, or design your own combination of tests.

For more information about how to use PerformanceTest, see the PerformanceTest online Help.

Start PerformanceTest

See "Install PerformanceTest" on page 59.

As part of installation, the PerformanceTest installer puts an icon on the Windows desktop.

To start PerformanceTest

❖ Do one of the following:
  - On the Windows desktop, double-click the PerformanceTest program icon.
  - On the Windows taskbar, click **Start** > **Programs** > **PerformanceTest** > **PerformanceTest**.

Access PerformanceTest Help

Help for PerformanceTest is accessible while you are running the program. Because PerformanceTest is a separate product, its help is not part of Norton SystemWorks Help.

To access PerformanceTest Help

1. Start PerformanceTest.
2. On the PerformanceTest Help menu, click **Help**.

6

Troubleshooting

Troubleshooting

22

Explore the Symantec service and support Web site

On the Symantec service and support Web site, you can find the latest protection and program updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

1. On the Internet, go to www.symantec.com/techsupp
2. On the service and support Web page, under the heading home & home office/small business, click **Continue**.
3. On the home & home office/small business page, click **start online support**.
4. Follow the links to the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

1. On the left side of any Symantec Web site page, click **search**.
2. On the search page, type a word or phrase that best represents the information for which you are looking. Use the following guidelines when searching the Symantec Web site:
   - Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type install to find articles that include the word install, installation, installing, and so on.
   - Type multiple words to find all occurrences of any of the words. For example, type virus definitions to find articles that include virus or definitions or both.
   - Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
   - Type a plus (+) sign in front of all of the search terms to retrieve documents containing all of the words. For example, +Internet +Security finds articles containing both words.
   - For an exact match, type the search words in uppercase letters.
   - To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, “purchase product”, “MAC”, “Norton SystemWorks” searches for all three phrases, and finds all articles that include any of these phrases.
3. Select the area of the Web site that you want to search.
4. Click **Search**.

Troubleshoot Rescue Disks

Check here for possible solutions to issues that might arise with Rescue Disks.

My Rescue Disk does not work

See "Create and use Rescue Disks" on page 86.

Due to the number of product-specific technologies used by manufacturers to configure and initialize hard drives, the Rescue program cannot always create a bootable disk automatically. If your Rescue Boot Disk does not work properly, do one of the following:

- Be sure you have downloaded the latest Rescue Disk update from LiveUpdate.
- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start from that disk. Remove the disk and insert your Rescue Boot Disk. At the DOS prompt, type **A:RSHELL**, press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.

Sometimes, your Rescue Boot Disk does not work properly because you have more than one operating system installed, such as Windows 2000 and Windows 98.

To modify your Rescue Boot Disk

1. Start up from your hard drive.
2. Insert your Rescue Boot Disk into drive A.
3. At the DOS prompt, type **SYS A:**
4. Press **Enter**.
   This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

I cannot start from drive A

See “Create and use Rescue Disks” on page 86.

If your computer does not check drive A first on startup, use your computer’s Setup program to change settings.

Be careful when making changes using your computer’s Setup program. If you have never used it before, you may want to refer to your computer manufacturer’s documentation.

To change your computer’s settings

1. Restart your computer.
   A message appears telling you the key or keys to press to run SETUP, such as Press <DEL> if you want to run SETUP.
2. Press the key or keys to launch the Setup program.
3. Set the Boot Sequence to boot drive A first and drive C second.
   Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program’s Help system, refer to the documentation that came with your system, or contact your system’s manufacturer.
4. Save the changes, then exit the Setup program.

You may need to use a special boot disk rather than the Rescue Boot Disk. In this case, use the boot disk or startup disk that came with your computer.

See “My Rescue Disk does not work” on page 301.

If your computer is set up with more than one operating system, such as Windows 2000 and Windows 98, you may need to modify the Rescue Boot Disk.

I get an error when testing basic Rescue Disks

See “Create and use Rescue Disks” on page 86.

If you get the message Non-system disk, replace the disk and press any key when testing your Rescue Disks, the Rescue program may not have prepared the floppy boot files correctly.

To repair the Rescue Boot Disk without having to reformat the disk and create a new Rescue Disk set

1. Remove the Rescue Boot Disk and restart your computer.
2. Insert the Rescue Boot Disk into the floppy disk drive.
3. On the Windows taskbar, click **Start** > **Run**.
4. In the Run dialog box, type **SYS A:**
5. Click **OK**.

Troubleshoot Norton SystemWorks

Check here for possible solutions to issues that might arise with Norton SystemWorks.

Use Norton GoBack to revert your disks

See "Revert your hard disk" on page 147.

If you are having problems due to a bad program installation or system crash and you installed Norton GoBack before the problems began, Norton GoBack can revert your hard disk to an earlier state. If you revert your hard disk, your data files will also revert to an earlier state.

Troubleshoot Norton Utilities

Check here for suggestions to help solve problems that are encountered while running Norton Utilities.

Norton Disk Doctor, Speed Disk, or other Norton Utilities keep restarting

Windows lets many applications access the hard drive simultaneously. When an application writes to the hard drive, the drive's directories change. Since some of the Norton Utilities programs, such as Norton Disk Doctor and Speed Disk, need up-to-date directory information, they must reread these structures any time that another application accesses the drive. To solve this problem, do one of the following:

- Close other applications that are accessing the disk.
- Start Windows without starting the applications that normally start by pressing Shift when you start Windows 98 or Windows Me. This restarts your computer in Windows Safe Mode.
- Disable any programs that are scheduled to run at regular intervals so that they do not start during a Norton Utilities operation.

My drive might not be configured properly

If Norton Disk Doctor or Speed Disk displays the message "Drive C: may not be configured properly," there are several items you can check.

Detailed procedures are provided in a Knowledge Base article titled "Error: Drive X: may not be configured properly when running Norton Disk Doctor or Speed Disk." To find this article, on the Internet, go to http://www.symantec.com/techsupp/

Troubleshoot disk errors in Windows 98/Me

See "Create and use Rescue Disks" on page 86.

Windows 98/Me are based on DOS (Disk Operating System), a command-line driven operating system. The CD includes four DOS-based Norton Utilities programs that you can use to diagnose and fix problems on your Windows 98/Me computer. Those programs are also available on the Emergency Disks and Rescue Disks that you can create from programs in Norton SystemWorks.

DOS procedures can be used on FAT16 or FAT32 volumes, but not on NTFS volumes.

The following DOS-based programs come with Norton Utilities:

- Norton Disk Doctor (NDD.EXE)
  Checks the integrity of logical disk structures and performs surface analysis tests to ensure the integrity of your disks.
  Diagnoses and repairs common disk problems.
- UnErase (UNERASE.EXE)
  Recovers erased files automatically or manually.
- UnFormat (UNFORMAT.EXE)
  Restores accidentally formatted disks or repairs a severely damaged disk.
- Disk Editor (DISKEDIT.EXE)
  Full-featured sector editor for advanced users that lets you manually examine and modify files, directories, clusters, sectors, and system areas of your disk. Use Disk Editor to edit, save, or undo changes to your disk parameters and to search an area of your disk for a particular data string.

DOS-based troubleshooting list

Many of the procedures that use DOS-based programs (Disk Editor, Norton Disk Doctor, UnErase, and UnFormat) require you to have a blank, formatted floppy disk available to create an Undo file, just in case the corrections you make are not what you expected.

For online information about the DOS-based Norton Utilities programs, you can press F1 on your computer keyboard while you use them.

Before you begin

The procedures for using the DOS-based programs require you to insert the Emergency Disk or Rescue Disk that has the program's .exe file. To save time, make directory printouts of your Emergency Disks and Rescue Disks so that you will know where the .exe files are located.

Some procedures recommend using either your Rescue Disk set or your Emergency Disks. If you have a Rescue Disk set, try that first, since your Rescue Disks have more up-to-date files for your computer. Otherwise, use the Emergency Disks.

DOS-based programs do not support NTFS formatted disks.

My computer displays an error message on startup

The following list includes many of the errors that you may see when you have problems starting your computer:

Parity error at address	See "Repair general hardware problems" on page 309.
ROM Checksum invalid	See "Repair general hardware problems" on page 309.
Seek error	See "Repair general hardware problems" on page 309.
Segment boundary overrun	See "Repair general hardware problems" on page 309.
Hard Drive # Controller failure, hard drive absent or missing	See "Repair general hardware problems" on page 309.

Faulty....	See "Repair general hardware problems" on page 309.
Illegal instruction trapped	See "Repair general hardware problems" on page 309.
HDD Controller Failure	See "Correct computer setup data" on page 310.
Hardware Information Lost	See "Correct computer setup data" on page 310.
Battery Discharged	See "Correct computer setup data" on page 310.
CMOS Checksum error	See "Correct computer setup data" on page 310.
CMOS Information not found	See "Correct computer setup data" on page 310.
Date and Time not set	See "Correct computer setup data" on page 310.
Disk Boot Failure	See "Correct computer setup data" on page 310.
Drive X error	See "Correct computer setup data" on page 310.
Hard Disk # error	See "Correct computer setup data" on page 310.
Memory Size Mismatch	See "Correct computer setup data" on page 310.
Unexpected amount of memory found	See "Correct computer setup data" on page 310.
No ROM BASIC – System halted	See "Recover startup data" on page 311.
Invalid Partition Table	See "Recover startup data" on page 311.
Invalid System Disk	See "Recover startup data" on page 311.
Missing Operating System	See "Recover startup data" on page 311.
Hard Disk Boot sector invalid	See "Recover startup data" on page 311.

Insert a (valid) boot disk	See "Recover startup data" on page 311.
Error loading Operating System (O/S)	See "Recover startup data" on page 311.

Repair general hardware problems

When you turn your computer on, it performs the Power-On Self Test (POST). This process verifies the existence and operation of hardware (hard drives, video hardware, memory, and the keyboard) that is critical to starting your computer. If a problem is found, it is reported to you on-screen or as a series of beeps if the video display is disconnected or not working. Refer to your computer manufacturer's documentation to decipher beep codes.

Many hardware problems that are found display messages similar to these:

- Faulty...
- Hard disk controller failure
- Hard disk absent or failed
- Illegal instruction trapped
- Parity error at address
- ROM checksum invalid
- Segment boundary overrun

Check inside your computer

Observe your computer manufacturer's safety guidelines before you open your computer. For proper handling instructions, refer to your computer manufacturer's documentation.

Before you suspect a defective device, check inside of your computer to ensure the following:

- Adapter cards, such as video and disk controller cards, are seated properly in the correct expansion slots.
- Memory modules are seated correctly.

- Drive cables are connected properly.
- Multiple hard drives are configured to work together. For more information on properly configuring multiple hard drives, refer to your computer manufacturer’s documentation as well as any documentation that you might have on your additional hard drives.
- Additional adapter cards, such as multimedia or tape backup controller cards, are configured properly. For information on properly configuring these devices, refer to the manufacturer’s documentation.

After you check these items, close the computer and turn it on to see if it starts normally.

If you cannot repair general hardware problems

If the problem persists, contact your computer manufacturer or the manufacturer of the device that you suspect is faulty.

Correct computer setup data

The POST process checks the settings of many hardware components against values that are stored in a CMOS chip. CMOS chips store vital information about your computer. Even when your computer is turned off, the CMOS chip continuously stores this information using a battery. If a discrepancy is found, a message similar to one of the following displays:

- Battery discharge
- CMOS checksum error
- CMOS information not found using defaults
- Date and time not set–run setup
- Drive <x> error
- Hard disk # error
- Hardware information lost–run setup
- HDD controller failure
- Memory size mismatch–run setup
- Unexpected amount of memory found–run setup

See “Recover startup data” on page 311.

The error may also be related to a partition table or *boot record* problem.

To correct computer setup data

1 Turn on your computer.

2 As your computer starts, press the key combination to enter the Setup program.
The correct key or key combination is usually shown on-screen as the computer starts.

3 Update the CMOS settings.
For more information, see your computer manufacturer’s documentation.
Many computers will update the CMOS with appropriate settings simply by running the Setup program and saving the values when you exit.

Recover startup data

When the POST process is complete, the hard drive is accessed for startup information if your A drive does not contain a disk. The first piece of startup information is the master boot record, which contains the partition table. The next piece of startup information is the boot record of the startup partition.

If any of the information in the master boot record, partition tables, or boot record is corrupt or missing, a message similar to one of the following displays:

- Hard disk boot sector invalid
- Please insert a boot disk
- Please insert a valid boot disk and press any key

You can recover startup data using Rescue Disks or Emergency Disks.

Never use Rescue Disks that were made on another computer. Rescue Disks contain information that is specific to the computer on which they were made. If you don’t have Rescue Disks, you can use Emergency Disks. See “To recover startup data with Emergency Disks” on page 312.

To recover startup data with Rescue Disks

1. Insert the Rescue Boot Floppy Disk into Drive A.
2. Turn on your computer and wait for the Rescue Disk screen to appear.
3. Use the DownArrow key to select **Rescue Recovery**, then press **Enter**.
   The Restore Rescue Information dialog box appears. Rescue Restore examines your computer's boot records and partition table information and automatically selects any damaged Rescue Restore items to be restored.

   If Rescue Restore does not detect any startup file problems, the Items To Restore check boxes will be unchecked. Do not proceed with the restore process. Press **Esc** to exit.
4. If Boot Records, Partition Tables, or both are selected, press **Alt+R** to restore the information.
   A confirmation box appears (twice) that lets you verify the information that you are about to restore.
5. Press **Enter** and follow the on-screen instructions.
6. Remove the disk from drive A and restart your computer.

If the problem has been fixed, your computer will start normally.

See "If your disk is damaged" on page 16.

You can use the CD as an Emergency Disk to scan with Norton AntiVirus if your computer can start from the CD-ROM drive.

Do not store undo data on the same physical drive that you are attempting to repair. The best place to store undo data is on a blank formatted floppy disk.

To recover startup data with Emergency Disks

1. Insert Emergency Disk 1 into drive A.
2. Restart your computer and wait for the Emergency Disk screen to appear.
3. Use the DownArrow key to select **Disk Doctor**, then press **Enter**.
4. At the prompt, type **/REBUILD**, then press **Enter**.

It is possible to damage your hard drive by using the /REBUILD switch. Be sure that you have backups of your data before you use this procedure.

5 Insert Emergency Disk 2 when it is requested.

6 In the Norton Disk Doctor main dialog box, press **Enter** to diagnose the drive.
A message indicates that your hard drive has no partitions.

7 Press **Enter** to have Norton Disk Doctor rebuild the partition table.
A message indicates that a partition has been found and asks you if you would like to revive it.

8 Do one of the following:
- If the indicated partition size is correct, press **Enter** to revive the partition table.
- If the indicated partition size is incorrect, click **No**.
- If you are unsure, click **Yes** and create an Undo file on another disk.
  Norton Disk Doctor continues to search.

9 Do one of the following:
- To revive more partition tables, press **Enter** to search for them.
- Press **Alt+N** to proceed.
  Before changes are made to the disk, you are prompted to create an Undo file.

10 Press **Enter** to create an Undo file.

11 In the Undo File dialog box, use the UpArrow and DownArrow keys to select the drive on which to store the Undo file.

12 Insert a formatted floppy disk with at least 100 KB of free space into drive A, then press **Enter**.

Do not reuse disks on which Undo files have been created. Overwriting the same disk with a newer Undo file prevents you from using earlier changes.

Norton Disk Doctor saves the Undo file to disk and repairs your partition tables. When Norton Disk Doctor has finished, a message indicates that the partition information has been changed.

13 Remove the disk from drive A and restart your computer.

If the problem has been fixed, your computer will start normally.

If you cannot recover startup data

See "To recover operating system files" on page 314.

If the problem persists, it is possible that the disk's operating system files are missing or corrupt.

Recover operating system files

When your computer successfully completes the POST process, your computer loads the master boot record program that passes control to the disk's boot record. The boot record then loads IO.SYS, which carries out the rest of the startup process. To start Windows, both COMMAND.COM and MSDOS.SYS files must be present. If they are not, your computer will not start Windows properly.

Before you recover operating system files, make sure that you have file-level access to the drive from the command prompt.

To recover operating system files

1. Insert the Rescue Boot Floppy Disk into drive A.
2. Turn on your computer and wait for the Rescue Disk screen to appear.
3. Press **Esc** to go to the DOS command prompt.
4. Insert NU Emergency Utility Disk 1, which contains the SYS.COM file, into drive A.
5. At the command prompt, type **SYS C:**, then press **Enter**.

   If the message "Insert system disk in drive A:\" appears, insert the Rescue Boot Floppy Disk into drive A and press any key.

   The SYS program copies the system files from your Rescue Disk to your hard drive.

6 Insert the Rescue Boot Floppy Disk, which contains the MSDOS.SAV file, into drive A.

7 At the command prompt, type
C:\WINDOWS\COMMAND\ATTRIB -R -S -H C:\MSDOS.SYS
If Windows is installed in a location other than C:\WINDOWS, modify the command line with the proper location (for example, C:\WIN95\COMMAND\ATTRIB -R -S -H C:\MSDOS.SYS).

8 At the command prompt, type
COPY A:\MSDOS.SAV C:\MSDOS.SYS, then press **Enter**.
Your MSDOS.SYS file is restored.

9 Remove the Rescue Disk from drive A and restart your computer.

If the problem has been fixed, your computer will start normally.

If you cannot recover operating system files

If the problem persists, it is possible that the disk itself has a problem. Consider reinstalling your Windows operating system from the Windows CD.

Recover corrupt registry files

If you have a problem with the registry, while you start your computer, you will receive a message similar to one of the following:

- Registry access error
- Warning: Windows has detected a registry or configuration error

Windows stores a backup of the registry files each time that you successfully start your system, so first try to have Windows restore the files by selecting the Restore From Backup And Restart button in the error message dialog box. If this fails to resolve the problem, restore the registry data from your registry backup, which is usually found in C:\WINDOWS\SYSTEM.RSC and C:\WINDOWS\USER.RSC.

There may be several backups of the SYSTEM and USER files, with *extensions* such as .NS0, .NS1, .SW0, or .NU0. Try all of these, in the order of newest to oldest.

When you are restoring the registry, always restore both of the registry files: System.dat and User.dat.

Try to restore the Windows registry with a backup copy that Windows made of the registry the last time that you successfully started your computer.

There is a potential for data loss when you restore the registry. You may lose settings for programs that have been installed and program options that have been saved since the backup of the registry was made.

To recover corrupt registry files with the Windows 98/Me registry backup

1. Start or restart your computer.
2. While “Starting Windows...” is on your screen, do one of the following:
   - Press and release **F8**.
   - Press and hold **Ctrl** while your computer starts.
3. In the startup window, select **Command Prompt Only**.
4. At the command prompt, change to the directory where Windows is installed (usually C:\WINDOWS). For example, type C: and press Enter. Then type CD \WINDOWS and press Enter.
5. Type the following commands, then press **Enter** after each one (system.da0 and user.da0 contain zeroes):
   ```
   attrib -h -r -s system.dat
   attrib -h -r -s system.da0
   attrib -h -r -s user.dat
   attrib -h -r -s user.da0
   ```
6. Rename system.dat and user.dat to system.bak and user.bak by typing the following commands, then pressing **Enter** after each one:
   ```
   ren system.dat system.bak
   ren user.dat user.bak
   ```

7. Type the following commands, then press **Enter** after each one:
   copy system.da0 system.dat
   copy user.da0 user.dat
8. Restart your computer.

If you are unable to restore the registry files with the Windows 98/Me registry backup, try using your Rescue Disks.

To recover corrupt registry files with Rescue Disks

1. Insert the Rescue Boot Floppy disk into drive A.
2. Turn on your computer and wait for the Rescue Disk screen to appear.
3. Press **Esc** to go to the DOS command prompt.
4. Change directories to C:\WINDOWS (or to the directory where Windows is installed).
   For example, if Windows is in C:\WINDOWS, type C:, then press Enter. Then type CD \WINDOWS, then press Enter.
5. Type the following commands, then press **Enter** after each one:
   command\attrib -h -r -s system.dat
   command\attrib -h -r -s user.dat
6. Rename system.dat and user.dat to system.bak and user.bak by typing the following commands, then pressing **Enter** after each one:
   ren system.dat system.bak
   ren user.dat user.bak
7. Type the following commands, then press **Enter** after each one:
   copy system.rsc system.dat
   copy user.rsc user.dat
8. Remove the Rescue Disk from drive A and restart your computer.

If the problem persists, reinstall Windows to recreate your Windows 98 or Windows Me registry files.

Troubleshoot problems with Disk Editor

The DOS-based Disk Editor program lets you do the following:

- Access data on a damaged floppy disk.
- Recover files on a disk that appears empty.
- Recover a formatted or severely damaged disk.
- Repair a disk with incorrect media descriptor byte information.
- Recover lost or damaged directories.
- Recover overwritten files.
- Recover corrupt registry files.
- Recover an inaccessible disk.

The *Norton SystemWorks User's Guide* PDF on the CD contains instructions for using Disk Editor. For more information, see "Access the User's Guide PDF" on page 94.

Troubleshoot Norton AntiVirus

Check here for possible solutions to issues that might arise with Norton AntiVirus.

Auto-Protect does not load when I start my computer

If the Norton AntiVirus Auto-Protect icon does not appear in the lower-right corner of the Windows taskbar, Auto-Protect is not loaded. There are three likely reasons that this is happening.

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

1. On the Windows taskbar, click **Start** > **Shut Down**.
2. In the Shut Down Windows dialog box, click **Restart**.
3. Click **OK**.

Norton AntiVirus may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Auto-Protect**.
3. Ensure that Start Auto-Protect when Windows starts up is checked.

Norton AntiVirus may not be configured to show the Auto-Protect icon in the tray.

To show the Auto-Protect icon in the tray

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Auto-Protect**.
3. Ensure that Show the Auto-Protect icon in the tray is checked.

I have scanned and removed a virus, but it keeps infecting my files

There are four possible reasons a virus could be reappearing.

The virus might be in a program file with an unusual extension for which Norton AntiVirus is not configured to look.

To reset Norton AntiVirus scanning options

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Manual Scan**.
3. Under Which file types to scan for viruses, click **Comprehensive file scanning**.
4. Click **Manual Scan** > **Bloodhound**.
5. Ensure that Enable Bloodhound heuristics is checked, then click **Highest level of protection**.
6. Click **OK**.
7. Scan all of the disks that you use and repair all infected files.

The source of the infection could also be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

See "If you need to use Rescue Disks to restore your system" on page 91.

Another reason could be that the virus is remaining in memory after you remove it from the *boot record*. It then reinfects your boot record. Use your Rescue Disks to remove the virus.

If the problem is a Trojan horse or worm that was transmitted over a shared network drive, you must disconnect from the network or password protect the drive to let Norton AntiVirus delete the problem.

Norton AntiVirus cannot repair my infected files

See "Keeping current with LiveUpdate" on page 169.

The most common reason that Norton AntiVirus cannot repair your infected files is that you do not have the most current virus protection on your computer. Update your virus definitions regularly to protect your computer from the latest viruses.

If after using LiveUpdate the virus still cannot be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

See "If Norton AntiVirus places files in Quarantine" on page 196.

- Quarantine the file and submit it to Symantec.
- If you don't need the file or a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

I can't receive email messages

There are several possible solutions to this problem.

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus.

Temporarily disable email protection. This might allow the problem email messages to download so that you can once again enable email protection. You are protected by Auto-Protect while email protection is disabled.

To temporarily disable incoming email protection

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under Internet, click **Email**.
3. Uncheck **Scan incoming Email**.
4. Click **OK**.
5. Download your email messages.
6. Reenable incoming email protection.

See "About System options" on page 120.

Your email client may have timed out. Make sure that timeout protection is enabled.

If you continue to experience problems downloading email messages, disable email protection.

To disable email protection

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under Internet, click **Email**.
3. Uncheck **Scan incoming Email**.
4. Uncheck **Scan outgoing Email**.
5. Click **OK**.

I can't send email messages

If you get the message Norton AntiVirus was unable to send your email message because the connection to your email server was disconnected, your email client may be set to automatically disconnect after sending and receiving mail.

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus.

For Norton AntiVirus to scan outgoing email messages for viruses, it intercepts and scans the messages before they are sent to your email provider. To resolve this issue, turn off this option within your email client. Consult your email client manual for instructions on how to do this, or disable Norton AntiVirus outgoing email scanning.

To disable outgoing email scanning

1. At the top of the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under Internet, click **Email**.
3. Uncheck **Scan outgoing Email**.
4. Click **OK**.

Troubleshoot Norton CleanSweep

Check here for suggestions to help solve problems that are encountered while you are running Norton CleanSweep.

I can't install Norton CleanSweep

If you have problems installing the Norton CleanSweep component of Norton SystemWorks over a previous version, you might need to disable the Fast & Safe Scheduler or recheck your system requirements.

- Installation issues
  You should disable the Fast & Safe Cleanup Scheduler before you reinstall or uninstall Norton CleanSweep. Do not install an earlier version of Norton CleanSweep over this version. If you want to install an earlier version of Norton CleanSweep, uninstall this version first, restart your computer, and then install the earlier version.

See "System requirements" on page 43.

- System requirements issues
  Check that your computer meets the minimum system requirements to install Norton SystemWorks. While most components of Norton CleanSweep might function correctly, you should not use Norton CleanSweep in a multiple processor environment.

I can't delete files that Norton CleanSweep has marked red

Items that are marked red indicate that their removal might endanger the stability of your computer's system files. Norton CleanSweep does not let you delete files that are marked red. You should not remove these files unless you are sure that they are not essential. To remove the files, use Windows Explorer.

I get an error message that Csinject is causing a problem

Csinject is one of the components of Smart Sweep. This file is necessary to monitor program installations. When Norton CleanSweep prompts you to close any programs that are running before you install a program, this component should not be closed.

The following are essential components of Smart Sweep:

- Csinsm32.exe
- Csinject.exe
- Csinsmnt.exe (Windows 2000/XP only)

Smart Sweep is not detecting any changes on any installation

Smart Sweep won’t detect any changes on installations when background applications are running. Close any applications that are running before you install the application that you want to monitor.

Troubleshoot Norton Password Manager

Check here for suggestions to help solve problems that are encountered while you are running Norton Password Manager.

I'm using Netscape (or Opera) and my product won't work

Norton Password Manager works with Microsoft Internet Explorer version 5.01 SP2 and later only.

I've forgotten my master password

This version of Norton Password Manager does not provide any way of recalling or displaying your master password. It is encrypted and has other security measures to prevent unauthorized people from finding it in the program. It is not recorded anywhere except on your computer, so Symantec Technical Support representatives will not be able to provide it to you. If you can't remember your password, you will have to set up a new profile and retype your private information.

Disk Editor

A

Disk Editor (DISKEDIT.EXE) is a DOS-based, full-featured, sector-editing tool that is capable of accessing virtually any area of a hard or floppy disk. You can edit files and directories, the partition table, the boot record, and the file allocation tables (FATs) on most hard disks. You can treat any group of clusters or sectors as an object to view and edit.

The procedures for using Disk Editor assume that you are familiar with the inner workings of disks. You must understand what you are doing before you edit any area of a disk. Otherwise, you could make the data on the disk inaccessible.

Start Disk Editor

Disk Editor is a DOS program. You can use it when you have restarted from previously created Rescue Disks or Emergency Disks.

See “Create and use Rescue Disks” on page 86 and “Create Emergency Disks” on page 25.

Disk Editor works on disks that have been formatted with the DOS FAT system. It is not designed to work with disks that have been formatted with NTFS file systems.

To start Disk Editor using Rescue Disks

See “Create and use Rescue Disks” on page 86.

1 Insert the Rescue Boot Floppy Disk into drive A.
2 Turn on your computer and wait for the Rescue Disk screen to appear.

3. Press **Esc** to go to the DOS command prompt.
4. Remove the Rescue Boot Floppy Disk.
5. Insert Emergency Utilities Disk 2, which contains the DISKEDIT.EXE file, into drive A.
6. At the command prompt, type **DISKEDIT**, then press **Enter**.

By default Disk Editor starts in read-only mode. You must start from an Emergency Disk or a Rescue Disk that restarts in DOS to change from read-only mode.

To start Disk Editor using Emergency Disks

1. Insert Emergency Disk 1 into drive A and restart your computer.
   The Emergency program runs in DOS.
2. Use the UpArrow and DownArrow keys to select **Disk Editor**.
3. At the command prompt, type **/W**
4. For program Help, press **F1** while you are running the program.

Change from read-only mode

You must change Disk Editor from its default read-only mode before you can save any changes that you make.

To change Disk Editor from read-only mode

1. Start Disk Editor from the DOS command line.
2. Type **DISKEDIT /W**
3. Press **Enter**.
4. When the Volume Lock message appears, press **Enter**.

Recover an unbootable hard disk

You may not be able to start from a hard disk for two major reasons:

- The first reason is the absence or corruption of the two *hidden* system files (IO.SYS and MSDOS.SYS for MS-DOS) or the absence or corruption of COMMAND.COM, the default command processor. If you have been using a third-party replacement (such as NDOS.COM, 4NT.EXE, or 4DOS.COM) for COMMAND.COM, corruption or absence of those files also can cause startup problems.
- The second reason is when the value of the partition table field that is called Boot is modified to “NO.” This tells Windows that a partition is not a startup partition, even if it is. Disk Editor can edit the partition table to mark a partition as the startup partition.

Recover an unbootable hard disk with Rescue Disks

See “Create and use Rescue Disks” on page 86.

If you have created Rescue Disks, you can use them to start your computer and then use Disk Editor to recover an unbootable hard disk.

If you have not created Rescue Disks, you can try to recover an unbootable hard disk using Disk Editor and Emergency Disks. See “Recover an unbootable hard disk with Emergency Disks” on page 330.

To recover an unbootable hard disk with Rescue Disks

1. Insert the Rescue Boot Floppy Disk into drive A.
2. Turn on your computer and wait for the Rescue Disk screen to appear.
3. Press **Esc** to go to the DOS command prompt.
4. Remove the Rescue Boot Floppy Disk.
5. Insert Emergency Utilities Disk 1, which contains the DISKEDIT.EXE file, into drive A.
6. At the command prompt, type **DISKEDIT /W**
7. Press **Enter**.

8 In the Volume Lock message, press **Enter**.

9 On the Object menu, click **Drive**

10 In the Select The Disk You Wish To Edit dialog box, select the disk with the partition that you want to mark as the startup partition, then press **Enter**.

11 In the Volume Unlock message, press **Enter**.

If you want to save changes to a disk, you must change from read-only mode every time you change to a new drive.

12 Click **Tools** > **Configuration**, then uncheck **Read Only**.

13 Press **Enter**.
Disk Editor scans the disk.

14 On the Object menu, click **Partition Table**.

15 Press **Y** to toggle the value in the Boot column to Yes.

16 On the Edit menu, click **Write Changes**.

17 In the Write Changes dialog box, click **Write**.

18 On the Object menu, click **Exit** to quit Disk Editor.

19 Restart your computer.

Recover an unbootable hard disk with Emergency Disks

See "Create Emergency Disks" on page 25.

You can recover an unbootable hard disk using Disk Editor and Emergency Disks. If you haven't already created Emergency Disks, you can use any computer to create them.

See "Recover an unbootable hard disk" on page 329.

If you created Rescue Disks, you should use them to recover an unbootable hard disk.

To recover an unbootable hard disk with Emergency Disks

1 Insert Emergency Disk 1 into drive A.

2 Turn on your computer and wait for the Norton Utilities screen to appear.

3 Use the UpArrow and DownArrow keys to select **Disk Editor**.

4 At the command prompt, type **/W**

5. Press **Enter**.
6. When you are prompted, insert Emergency Disk 2, then press **Enter**.
7. On the Object menu, click **Drive**.
8. In the Select The Disk You Wish To Edit dialog box, select the disk with the partition that you want to mark as the startup partition, then press **Enter**.

> If you want to save changes to a different drive while you are using Disk Editor, make sure that read-only mode is turned off.

9. To edit or save changes to a different drive, click **Tools** > **Configuration**, then uncheck **Read Only**.
10. On the Object menu, click **Partition Table**.
11. Press **Y** to toggle the value in the Boot column to Yes.
12. On the Edit menu, click **Write Changes**.
13. In the Write Changes dialog box, click **Write**.
14. On the Object menu, click **Exit** to quit Disk Editor.
15. Restart your computer.

Recover lost subdirectories from a corrupt directory

Directories are special kinds of files that contain file and directory information. Directories can become corrupted and unreadable if the cluster that they reside in is damaged.

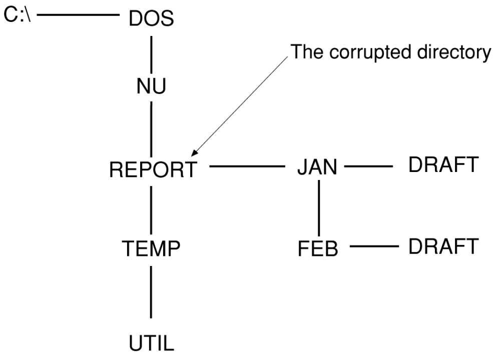
When a directory is unreadable, the files and directories that it contains are inaccessible. Norton Disk Doctor considers them to be lost clusters instead of files and directories.

About directory structure

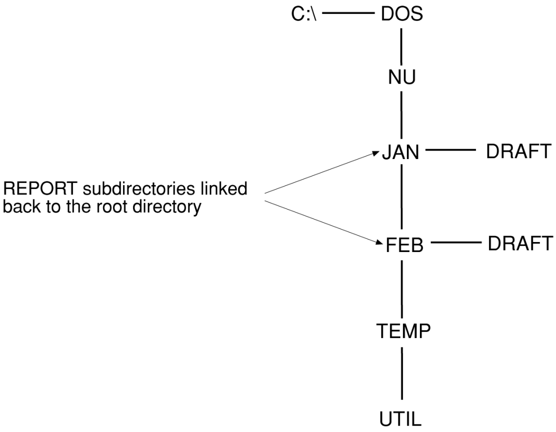
The Sample directory structure below shows a directory structure before one of its directories, REPORT, becomes unreadable.

Sample directory structure

Assume that the cluster that the REPORT directory occupies is physically damaged and is no longer readable. All of the directories and files that are contained in REPORT are inaccessible. Disk Editor can link the lost directories back to the root directory, as shown in the Repaired directory structure.



Repaired directory structure



Recovery methods

Track information on paper as you complete the following procedures by creating three columns. Label them as follows:

- Corrupt directory cluster number
- Good sectors
- Lost directories

To recover subdirectories from a corrupt directory, use the following procedures.

Action	For more information
Locate clusters for the corrupt directory.	See "To locate the cluster for the corrupt directory" on page 334.
Find readable sectors.	See "To find all of the readable sectors" on page 335.

Action	For more information
Copy good entries to the root directory.	See "To copy the good entries to the root directory" on page 335.
Find lost directories.	See "To find lost directories" on page 336.
Link lost directories to the root directory.	See "To link the lost directories to the root directory" on page 337.
Adjust parent directory pointers.	See "To adjust the parent directory pointers within each recovered directory" on page 337.

To locate the cluster for the corrupt directory

See "Start Disk Editor" on page 327.

1. Start Disk Editor.
2. On the Object menu, click **Drive**.
3. In the Select The Disk You Wish To Edit dialog box, select the drive with the corrupt directory, then press **Enter**.
   Disk Editor scans the disk.
4. On the Object menu, click **Directory**.
5. In the Change Directory dialog box, select the parent of the corrupt directory, then press **Enter**.
6. In the Directory View, select the corrupt directory, then press **Enter**.
   In most cases, you get read errors immediately after you press Enter. Usually only one or two sectors that make up the cluster are damaged, which lets you read the remaining good sectors. The good sectors cut down your workload, since you can copy the data that is within them to the root directory.
   You will have to re-create the data in the corrupt sectors. See "To find lost directories" on page 336.
7. Record the number in the Cluster field for the corrupt directory's entry on your piece of paper in the Corrupt directory cluster number column.
   Disk Editor tries to read the cluster that the corrupt directory occupies.

Usually only one or two sectors are damaged, which lets you read the remaining good sectors.

To find all of the readable sectors

1. If you immediately get a read error from Disk Editor, press **Enter** to clear the message.
2. Press **PageDown** to read the next sector of the cluster.
3. Record the good sector number on your piece of paper in the Good sectors column.
   The current sector number is displayed at the beginning of each sector in logical mode.
4. Continue pressing **PageDown** until you reach the end of the cluster or cannot advance past the read errors.

Using the good sector numbers, you can relocate the valid entries to the root directory.

To copy the good entries to the root directory

See "Start Disk Editor" on page 327.

1. Start Disk Editor.
2. On the Object menu, click **Sector**.
3. In the Select Sector Range dialog box, type the first sector number from your "Good sectors" list into the Starting Sector and Ending Sector text boxes, then press **Enter**.
   Disk Editor displays the sector in Directory View.
4. On the View menu, click **As Directory**.
5. On the Edit menu, click **Mark**.
6. Select all of the valid entries and exclude entries labeled Unused Directory Entry.
7. On the Edit menu, click **Copy** to copy the selected entries to the Disk Editor Clipboard.
8. On the Object menu, click **Directory**.
9. In the Change Directory dialog box, press **Enter** to select the root directory.
   Disk Editor displays the root directory in Directory View.
10. Select the first entry labeled **Unused Directory Entry**.

11 On the Edit menu, click **Paste Over** to append the directory entries from the Disk Editor Clipboard to the root directory.

12 On the Edit menu, click **Write Changes**.

13 Repeat steps 2 to 12 for all of the sectors that you recorded.

Use Disk Editor to locate all of the top-level directories that you want to recover. Once the directories are found, Disk Editor can link them back to the root directory.

To find lost directories

See "Start Disk Editor" on page 327.

1 Start Disk Editor.

2 On the Object menu, click **Cluster**.

3 In the Select Cluster Range dialog box, in the Starting Cluster text box, type **2**, then press **Enter**.

4 On the Tools menu, click **Find Object** > **Subdirectory**.
Disk Editor searches for the cluster string.

5 When Disk Editor finds the search string, on the View menu, click **As Directory**.

6 Do one of the following:

- If the screen does not resemble the contents of a directory, on the Tools menu, click **Find Again** until the information on the screen does resemble a directory.
- If the screen does resemble a directory, look at the number in the Cluster field for the ". .   " (two periods followed by six spaces) entry. If this number is the same as the number that you recorded for the Corrupt directory cluster number, record the number next to the Cluster label on the status line on your piece of paper in the Lost directories column.

7 On the Tools menu, click **Find Again** and repeat step 6 to search for additional lost directories until you locate all of the top-level child directories that you want to recover.

Once lost directories are found, Disk Editor can link them back to the root directory.

To link the lost directories to the root directory

See "Start Disk Editor" on page 327.

1. Start Disk Editor.
2. On the Object menu, click **Directory**.
3. In the Change Directory dialog box, select the root directory, then press **Enter**.
   Disk Editor displays the root directory in Directory View.
4. Select the first entry labeled **Unused Directory Entry**.
5. In the Name field, type a unique name for the current top-level directory.
6. In the Size field, type **0**
7. In the Date and Time fields, type the current date and time.
8. In the Cluster field, type the cluster number for the lost directory that you are currently working with from the Lost directories column.
9. With the cursor in the D column, press the SPACEBAR to toggle the directory attribute on.
10. Repeat steps 2 to 9 for all of the lost directories in the Lost directories column.
11. On the Edit menu, click **Write Changes**, then press **Enter**.
12. In the Write Changes dialog box, click **Write**.
    You have recovered the directories.

Disk Editor allows you to rebuild the directory structure by adjusting the directory pointers within each recovered directory.

To adjust the parent directory pointers within each recovered directory

1. Select one of the recovered directory entries, then press **Enter**.
   You should see the contents of the directory with the first two entries being "." and "..".
2. In the Cluster field for the ".." entry, type **0**
3. On the Edit menu, click **Write Changes**, then press **Enter**.

4 In the Write Changes dialog box, press **Enter** to write the change.

5 Select the ".." entry again, then press **Enter**.
This confirms the link by returning you to the root directory and puts you where you need to be for the next recovered directory.

6 Repeat steps 1 to 5 for each of the recovered directories.

Use Norton Disk Doctor to clean up any lost clusters that were left on your disk. If you save the lost clusters as files, you can examine them and recover any additional lost files. Simply rename the files that you want and delete the rest. Norton Disk Doctor uses the file naming scheme FILE0000._DD, FILE0001._DD, and so on for the file names that represent lost clusters.

Now that you have recovered the directories, re-create the directories that they originally resided in and move them back. You do not have to worry about the directories being re-created in the same spot. Windows now avoids the bad area on the disk.

Lift data from a damaged hard disk

Extracting data from a disk is a time-consuming process, so you should only try to recover files that you have not backed up or do not have copies of elsewhere. Reinstall any program files from their original disks rather than trying to recover them with Disk Editor from a corrupt hard disk.

Neither Windows nor Norton Disk Doctor can access a corrupt disk. However, Disk Editor can access most bad disks and let you lift the data that they contain.

About bad disk problems

There are two classes of bad disk problems:

Logical problems	Involve write errors that result in scrambled data on the disk. Fortunately, Norton Disk Doctor fixes most of these problems for you automatically.
Physical problems	Usually involve physically damaged sectors in the partition table, boot record, the first copy of the file allocation table (FAT), any combination of these system areas, or even the entire disk. When sectors in the system areas become physically damaged, Windows cannot access the disk normally. Since Norton Disk Doctor usually cannot repair physically damaged sectors, you may never gain normal access to a disk with damaged sectors in the system area unless you perform a low-level format. However, traditional low-level formatters for older hard disks destroy the existing data and do not work with today's sector-translating IDE, SCSI, and ESDI hard disks. If the disk is physically damaged, it will need to be repaired by a qualified service center.

Error 129 indicates that a disk is physically damaged and that no recovery is possible using Norton Utilities DOS tools.

Disk Editor classifies a disk as either a logical or a physical disk. If a disk can be accessed as a logical disk, Disk Editor uses clusters, which are usually composed of four or more sectors, as the smallest data allocation units. This makes manual recovery easier. Disk Editor treats severely damaged disks as physical disks automatically.

Disk Editor lets you access data around the damaged areas, cluster by cluster, file by file. This way, you can recover critical data files that you have not backed up and cannot do without.

Data recovery procedures

To lift data from a corrupt or physically damaged hard disk, use the following procedures.

Action	For more information
Identify the disk type.	See "Determine whether Disk Editor is accessing your disk as a logical or physical disk" on page 340.
If the disk is being accessed as a logical disk, extract data.	See "Extract data from a logical disk" on page 341.
If the disk is being accessed as a physical disk, extract clusters.	See "Extract clusters from a physical disk" on page 342.
Find more lost clusters.	See "Find the rest of the clusters" on page 346.

Once you fix the problem, make sure that a virus is not causing it.

Determine whether Disk Editor is accessing your disk as a logical or physical disk

Disk Editor estimates the correct values of your disk's physical and logical parameters. The number of sides, cylinders, sectors, and so on are inserted into the appropriate fields of the Advanced Recovery Mode dialog box automatically and used to treat the disk as a logical disk.

If the disk's parameters are incorrect, the resulting logical disk may have structural problems. If you consistently run into problems accessing the disk, reenter the disk's physical and logical parameters in the Advanced Recovery Mode dialog box. For example, if you select the first copy of the FAT but do not see it, the number of total sectors may be incorrect.

To determine whether Disk Editor is accessing your disk as a logical or physical disk

See "Start Disk Editor" on page 327.

1. Start Disk Editor.
2. On the Object menu, click **Drive**.
3. In the Select The Disk You Wish To Edit dialog box, in the Type box, click **Logical Disks**.
4. Do one of the following:
   - If the bad disk can be accessed as a logical disk, the disk is listed in the drives list box and you can proceed. See "Extract data from a logical disk" on page 341.
   - If the bad disk is not listed in the drives list box, continue to the next step.
5. On the Tools menu, click **Advanced Recovery Mode**.
6. In the Advanced Recovery dialog box, press **Alt+R**.
7. In the Select The Disk You Wish To Review dialog box, select the bad disk, then press **Enter**.
8. In the Advanced Recovery dialog box, press **Alt+V**.
   Disk Editor rescans the disk as a logical disk. When scanning is complete, you should see the root directory of the disk in Directory View.

⚠ If you cannot see the root directory of the disk in Directory View, do not continue. The following procedures will not work.

Extract data from a logical disk

If Disk Editor can access your bad disk as a logical disk directly or by using Advanced Recovery Mode, use the following procedure. To recover a file, you must find, select, and write it out to another disk.

To extract data from a logical disk

See "Start Disk Editor" on page 327.

1. Start Disk Editor.
2. On the Object menu, click **Directory**.
3. In the Change Directory dialog box, select the directory that contains the file that you want to recover, then press **Enter**.
   The directory listing appears in Directory View.

4. Find the file in the directory listing, then do one of the following:
   - If the file exists, continue to step 5.
   - If the file does not exist in this directory, try looking in other directories.
5. Select the name of the file that you want to recover, then press **Enter**.
   The contents of the file appear in Hex View.
6. On the Tools menu, click **Write Object To**.
7. In the Write dialog box, select **To A File**, then press **Enter**.
   The Save dialog box appears.
8. Remove your disk from drive A and insert the disk to which you want to write.
9. In the text box, type a drive letter followed by a file name, then press **Enter**.
10. In the confirmation box, click **Yes** to write the file out.
    A "Copying…" progress box appears for the duration of the copy function.
11. Repeat steps 2 to 10 for each of the files that you want to recover.

Extract clusters from a physical disk

When Disk Editor cannot access the disk as a logical disk, you can still lift individual clusters, starting with the first cluster of the file. This is possible because Disk Editor can work with clusters instead of sectors.

To extract clusters from a physical disk

❖ Try each of the following methods in the order in which they are listed:

Search for the file name.	See "Method 1: Find the starting cluster by searching for the file name" on page 343.
Browse all directories.	See "Method 2: Find the starting cluster by browsing all of the directories" on page 344.
Search for text within a file.	See "Method 3: Search for unique text in the file" on page 345.

Method 1: Find the starting cluster by searching for the file name

When the directory structure of a disk is still intact, you can find the starting cluster number by searching the disk for the directory entry of the file, which contains the starting cluster number.

To find the starting cluster by searching for the file name

See "Start Disk Editor" on page 327.

1 Start Disk Editor.

2 On the Object menu, click **Cluster**.

3 In the Select Cluster Range dialog box, in the Starting Cluster text box, type **2**, then press **Enter**.

4 On the Tools menu, click **Find**.

5 In the Enter Search Text dialog box, in the ASCII text box, type the file name, then press **Enter**.
Do not type the file name in the regular format. Instead, type the file name followed by enough spaces to make eight characters. Then, type the file extension as the next three characters. Do not put a period between the name and the extension. For example, type NAME.EXT as:
NAME****EXT (do not type the asterisks)
There are four spaces between NAME and EXT because NAME has four characters already. The Search Progress dialog box appears. Disk Editor finds

the search string, selects it, and displays it in Hex View.

6 On the View menu, click **As Directory** to switch to Directory View.

7 Do one of the following:

- If the data that you see appears to be a directory, record the file name, starting cluster number, and file size of the file from those fields on a piece of paper that is labeled Files To Recover.
  The starting cluster number is the number in the Cluster field on the same line as the file name.
- If the data contains unrecognizable characters, such as happy faces, hearts, and other nonstandard characters, on the Tools menu, click **Find Again** to search for another occurrence of the file name.

8 Find and record the starting cluster numbers and file sizes for all of the files that you want to recover.

See "Find the rest of the clusters" on page 346.

9 Find the rest of the clusters for each file.

Method 2: Find the starting cluster by browsing all of the directories

You can locate the file that you want to recover by browsing all of the directories on the disk. To locate all of the directories on the disk except the root directory, search for "..   " (two periods followed by six spaces). Every directory other than the root has "..   " as its second entry. As you find each directory, scan the directory listing for the file that you want to recover.

To find the starting cluster by browsing all of the directories

See "Start Disk Editor" on page 327.

1 Start Disk Editor.

2 On the Object menu, click **Cluster**.

3 In the Select Cluster Range dialog box, in the Starting Cluster text box, type **2**, then press **Enter**.

4 On the Tools menu, click **Find Object** > **Subdirectory**.
The Search Progress dialog box appears.

5 Once the search completes, on the View menu, click **As Directory** to switch to Directory View.

6 Do one of the following:
   - If the display is a directory and the file that you want to recover is listed, record the name, starting cluster number, and size of that file on a piece of paper that is labeled Files To Recover.
   - If the display is not a directory or you cannot locate the file that you want to recover, on the Tools menu, click **Find Again** to continue searching for more directories.

See "Method 3: Search for unique text in the file" on page 345.

If this method is unsuccessful, try searching for a unique text string that appears in the starting cluster of the file.

Method 3: Search for unique text in the file

When the directory structure is damaged, the best way to find the starting cluster is to search for embedded text in the starting cluster. This method works best for text files such as word processing files.

To search for unique text in the file

See "Start Disk Editor" on page 327.

1 Start Disk Editor.

2 On the Object menu, click **Cluster**.

3 In the Select Cluster Range dialog box, in the Starting Cluster text box, type **2**, then press **Enter**.

4 On the Tools menu, click **Find**.

5 In the Enter Text To Search For dialog box, in the ASCII text box, type a unique string that appears at the beginning of the file, then click **Find** to begin the search.
For example, if you are looking for a word processor file with the title Year End Report, type the string Year End Report in the text box.
If it is found, Disk Editor displays the search string in Hex View.

6 On the View menu, click **As Text** to switch to Text View.

7 Do one of the following:
   - If the cluster that contains the string appears to be the first cluster in the file, record the starting cluster's number and a name for the file on a piece of paper that is labeled Files To Recover. Mark the number and name as the starting cluster.
   - If the cluster that contains the string belongs to the file but does not appear to be the first cluster, record the cluster number on the same piece of paper next to the file name. Do not mark the number as the starting cluster.
   - If the cluster with the search string does not belong to the file that you are looking for, on the Tools menu, click **Find Again** to continue the search. If you have not found any clusters from your file, try searching for a different text string.

Find the rest of the clusters

Now that you have found the starting cluster, you need to find the rest of the clusters in the file.

- If you found the starting cluster, the file name, and the file size using method one or method two in "Extract clusters from a physical disk" on page 342, see "Method 1: Find the rest of the clusters with the file size" on page 346.
- For any other methods that you used, see "Method 2: Find the rest of the clusters without the file size" on page 348.

Method 1: Find the rest of the clusters with the file size

With the file size, you can calculate the number of clusters that the file contains. Then you can locate and record the individual clusters that you later write out to a file.

To find the rest of the clusters with the file size

See "Start Disk Editor" on page 327.

1 Start Disk Editor.

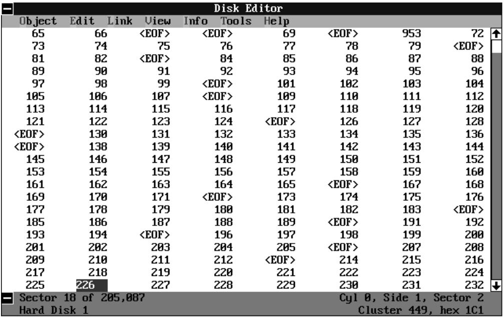
2 On the Info menu, click **Drive Info**.

3 In the Drive Info dialog box, multiply the values for Bytes Per Sector and Sectors Per Cluster.
The result is the size of each cluster in bytes.

4 Divide the file size by the cluster size.

5 Round off the value to the next integer value.
For example, if the file size is 100,000 bytes and your disk's cluster size is 8,196 bytes, the file has 13 clusters (12.2 rounded up to 13).

6 On the Object menu, click **1st FAT**.
If you cannot find the FAT or if it is very corrupt, continue to step 7.



```
     65        66     <EOF>     <EOF>        69     <EOF>       953        72
     73        74        75        76        77        78        79     <EOF>
     81        82     <EOF>        84        85        86        87        88
     89        90        91        92        93        94        95        96
     97        98        99     <EOF>       101       102       103       104
    105       106       107     <EOF>       109       110       111       112
    113       114       115       116       117       118       119       120
    121       122       123       124     <EOF>       126       127       128
  <EOF>       130       131       132       133       134       135       136
  <EOF>       138       139       140       141       142       143       144
    145       146       147       148       149       150       151       152
    153       154       155       156       157       158       159       160
    161       162       163       164       165     <EOF>       167       168
    169       170       171     <EOF>       173       174       175       176
    177       178       179       180       181       182       183     <EOF>
    185       186       187       188       189     <EOF>       191       192
    193       194     <EOF>       196       197       198       199       200
    201       202       203       204       205     <EOF>       207       208
    209       210       211       212     <EOF>       214       215       216
    217       218       219       220       221       222       223       224
    225       226       227       228       229       230       231       232
 Sector 18 of 205,087                           Cyl 0, Side 1, Sector 2
 Hard Disk 1                                       Cluster 449, hex 1C1
```

EOF markers

7 Use the PageDown and Tab keys until the Cluster label on the status line matches the starting cluster number of the file that you want to recover.
When you find the starting cluster, its position on the screen (not Disk Editor's status line) should display <EOF>, which marks the last cluster in the file or the number for the next cluster. If it is marked <EOF>, you have found the first and last cluster of the file. You can write the cluster to disk. See "To write the clusters to disk" on page 350.

8 If the cluster label has the cluster number of the next cluster in the file, use the PageDown and Tab keys to move to that cluster and select it.

Remember to use the Cluster label on the status line as the cluster number reference.

9 Record the number that is indicated by the Cluster label on the status line next to the file name on your Files To Recover list.
Unless the file is composed of multiple cluster chains, the next cluster is usually immediately to the right of the current cluster. If this cluster position is marked with <EOF>, it is the last cluster of the file. You can write the cluster to disk. See "To write the clusters to disk" on page 350.

10 Continue finding and recording clusters for the file until you find the <EOF> marker.

11 Compare the number of clusters that you recorded from the FAT with the number that you calculated earlier (by dividing the file size by the cluster size), then do one of the following:
   - If they are not the same, double-check your calculations or try this procedure again.
   - If they are the same, you can write the clusters to disk. See "To write the clusters to disk" on page 350.

Method 2: Find the rest of the clusters without the file size

Unless the disk is very *fragmented*, the rest of the clusters of the file should be near and after the starting cluster. Locate the rest of the file by browsing near the starting cluster or search for text that appeared somewhere after the starting cluster. This procedure works best for text files.

To find the rest of the clusters without the file size

See "Start Disk Editor" on page 327.

1 Start Disk Editor.

2 On the Object menu, click **Cluster**.

3 In the Select Cluster Range dialog box, in the Starting Cluster text box, type the starting cluster number from your Files To Recover list, then press **Enter**.
Disk Editor displays the contents of the starting cluster in Hex View.

4 On the View menu, click **As Text**.

5. Scroll to the next cluster using the PageDown and DownArrow keys.
   The cluster markers on the screen (not on the status line) differentiate cluster numbers.
6. When you find a cluster that belongs to the file, record the cluster number that is displayed next to the Cluster label on the status line on your Files To Recover list.
   Record the number next to the name of the file to which the cluster belongs.
7. Using the data in the newest cluster to figure out what should be in the next cluster, continue browsing for clusters until you have found the expected number of clusters for the original file.
8. Do one of the following:
   - If you have found all of the clusters from the original file, write the clusters to a new location. See “To write the clusters to disk” on page 350.
   - If you could not locate additional clusters near the starting cluster, continue the search by searching for text. See “To search for text on the disk” on page 349.
9. Press **Home** once.
   Disk Editor returns to the starting cluster.

To search for text on the disk

See “Start Disk Editor” on page 327.

1. Start Disk Editor.
2. On the Tools menu, click **Find**.
3. In the Enter Search Text dialog box, in the ASCII text box, type the text to search for, then select **Find** to begin the search.
4. When the search string is found, record the cluster number that contains the search string if the number belongs to the file on your Files To Recover list.
5. Record the number next to the name of the file to which the cluster belongs.
6. Start a new search for text that you expect to be in the next cluster or manually browse the next several clusters for the next cluster using the PageDown and DownArrow keys.

7 If no clusters are found, on the Tools menu, click **Find**, then type a new search string.

8 Continue searching until you have reached the expected end of the file.

To write the clusters to disk

See "Start Disk Editor" on page 327.

1 Start Disk Editor.

2 On the Object menu, click **Cluster**.

3 In the Select Cluster Range dialog box, in the Starting Cluster and Ending Cluster text boxes, type the starting cluster number of the first file name from your Files To Recover list, then press **Enter**.

4 On the Tools menu, click **Write Object To**.

5 In the Write dialog box, select **To A File**, then press **Enter**.
The Write Object To File dialog box appears.

6 Insert a blank floppy disk into drive A or drive B.

7 Type the drive letter of the drive that contains the blank floppy disk, followed by a file name for the file that was created with the clusters that you have found, then press **Enter**.
For example, A:MYFILE.DOC.
A confirmation dialog box appears that asks if you want to write the file out.

8 Click **Yes**.
The write progress screen appears for the duration of the write operation.

9 Repeat steps 2 through 7 for each cluster in your Files To Recover list and when you get to step 7, use the same file name.
This causes a message box to appear, which tells you that the file already exists.

10 Press **Enter** to append the file.

Repair cross-linked files

When Norton Disk Doctor or ScanDisk examines a disk, it might report that two or more files are cross-linked. When two or more (usually only two) files are cross-linked, they are sharing the same cluster or chain of clusters. The cross-linkage can take place anywhere along the cluster chain, not just on the first or last cluster.

Since each cluster can only belong to one file at a time, one of the cross-linked files is unusable until you eliminate the cross-linkage. Furthermore, one of the cross-linked files is almost always the real owner of the cross-linked clusters. Usually, you can recover the missing clusters for the other file as lost clusters and link them into the correct file.

First, you need to identify the files that are cross-linked and the clusters on which they are cross-linked.

To repair cross-linked files

❖ Do one of the following:

- See “To identify and recover cross-linked files with Norton Disk Doctor” on page 351.
- See “To examine the clusters to see where they belong” on page 354.
- See “To link a _DD or CHK file back to the corrupt file to which it belonged” on page 354.

If you cannot access Windows or your computer will not start, you can try using Emergency Disks. See “To identify cross-linked files with Norton Disk Doctor and Emergency Disks” on page 352.

This procedure helps you identify matching parts of cross-linked files.

To identify and recover cross-linked files with Norton Disk Doctor

See “Check your disk with Norton Disk Doctor” on page 206.

1 In the Norton Disk Doctor main window, check the disk to diagnose, then click **Diagnose**.

2 Follow the on-screen instructions to continue.

Do not make any corrections to the disk yet.

3 When Norton Disk Doctor locates the cross-linked files, record their names.

4. Copy the cross-linked files to another disk.
   If a file is too big, you can copy it to another directory, though this is not recommended.
5. Verify whether the files that you copied (not the original file) are corrupt, then do one of the following:
   - For a data file, open it with the application that created it (or one that recognizes the type of data in the file).
   - For a program file, try running it.
6. Delete the cross-linked files from the original disk.
7. Copy the good files back to the same directory of the original disk.
8. Copy the corrupt files back to the same directory of the original disk.
9. In Norton Disk Doctor, check the drive to diagnose, then click **Diagnose**.
10. Follow the directions to continue and let Norton Disk Doctor make any necessary corrections to the disk.
    Norton Disk Doctor saves chains of lost clusters to the root directory as files with _DD extensions. For example, five lost cluster chains would be saved as FILE0000._DD, FILE0001._DD, and so on to FILE0004._DD. ScanDisk uses the same naming convention as Norton Disk Doctor, except the extension CHK is used instead of _DD.
11. Examine the clusters.
    See “To examine the clusters to see where they belong” on page 354.

To identify cross-linked files with Norton Disk Doctor and Emergency Disks

1. Insert Emergency Disk 1 into drive A.
2. Turn on your computer and wait for the Norton Utilities screen to appear.
3. Use the UpArrow and DownArrow keys to select **Norton Disk Doctor**, then press **Enter**.
4. In the Norton Disk Doctor main window, press **Enter** to diagnose the disk.
5. In the Select Drives To Diagnose dialog box, select the drive to diagnose, then press **Enter**.

6 Follow the on-screen instructions to continue.

Do not make any corrections to the disk yet.

7 When the cross-linked files are located, record their names.

8 Copy the cross-linked files to another disk.
If a file is too big, you can copy it to another directory, though this is not recommended.

9 Verify whether the files that you copied (not the originals) are corrupt, then do one of the following:

- For a data file, open it with the application that created it (or one that recognizes the type of data in the file).
- For a program file, try running it.

10 Delete the cross-linked files from the original disk.

11 Copy the good files back to the same directory of the original disk.

12 Copy the corrupt files back to the same directory of the original disk.

13 Turn off your computer.

14 Insert Emergency Disk 1 into drive A.

15 Turn on your computer and wait for the Norton Utilities screen to appear.

16 Use the UpArrow and DownArrow keys to select **Norton Disk Doctor**, then press **Enter**.

17 In the Norton Disk Doctor main window, click **Diagnose Disk**, then press **Enter**.

18 In the Select Drives To Diagnose dialog box, select the drive to diagnose, then press **Enter**.

19 Follow the on-screen instructions to let Norton Disk Doctor make any necessary corrections to the disk.
Norton Disk Doctor saves chains of lost clusters to the root directory as files with _DD extensions. For example, five lost cluster chains would be saved as FILE0000._DD, FILE0001._DD, and so on to FILE0004._DD. ScanDisk uses the same naming convention as Norton Disk Doctor, except the extension CHK is used instead of _DD.

To examine the clusters to see where they belong

See "Start Disk Editor" on page 327.

1 Start Disk Editor with the /W command-line option.

2 On the Object menu, click **Drive**.

3 In the Select The Disk You Wish To Edit dialog box, select the disk that contains the _DD or CHK files using the UpArrow and DownArrow keys, then press **Enter**.
The root directory of the disk displays in Directory View. You may not see the _DD or CHK file in the directory listing immediately.

4 Use the UpArrow and DownArrow keys to locate the files.
Use the PageUp and PageDown keys to scroll a screen at a time.

5 Select a _DD or CHK file, then press **Enter**.
The contents of the file appear in Hex View.

6 If the file is a text file, on the View menu, click **As Text**.

7 If you know which corrupt file the data belongs to, do one of the following:
   - On the Link menu, click **Directory** to return to the root directory.
   - Select another _DD or CHK file.

8 Record the file name, file size, and starting cluster number of the _DD or CHK file on a piece of paper.
The starting cluster number for each _DD or CHK file is in the Cluster field on the same line as the _DD or CHK file name.

9 Repeat steps 5 through 8 for each of the _DD or CHK files in your root directory.

To link a _DD or CHK file back to the corrupt file to which it belonged

See "Start Disk Editor" on page 327.

1 Start Disk Editor with the /W command-line option.

2 On the Object menu, click **Directory**.

3 In the Change Directory dialog box, select the directory that contains the corrupt file, then press **Enter**.
The directory appears.

4 Select the corrupt file, then press **Enter**.
The file is displayed in Hex View.

5 Scroll through the file until you notice a discontinuity.

6 Note the cluster that the cursor is in by using the value in the status bar, then press **Enter** to return to the directory.

7 Add the size of the _DD or CHK file to the size of the corrupt file and, in the Size text box, type the total for the corrupt file.

8 Press **Ctrl+W** to write the changes, then click **Write**.

9 Press **Ctrl+T** to view the cluster chain for the file.

10 Select the cluster that is noted on the status line in step 6 and note its value.

11 Type the cluster number that you recorded on paper for the _DD or CHK file here, then press **Ctrl+W**.

12 Make sure that Synchronize FATs is checked in the dialog box, then click **Write**.

13 In the Rescan dialog box, click **Cancel**.

14 Move the cursor to the cluster for the _DD or CHK file in the current view.

15 Use the Tab and DownArrow keys to scroll through the cluster chain for this file until you reach <EOF>.

16 Change <EOF> to the value that was noted in step 10.

17 Press **Ctrl+W**, then press **Enter**.

18 In the Rescan dialog box, on the Object menu, click **Directory**.

19 In the Change Directory dialog box, select the root directory, then press **Enter**.

20 Move to the Name field of the _DD or CHK file, then press **F2** to display the Hexadecimal view.

21 Without moving the cursor, type **E5**

22 Press **Ctrl+W** to write the change, then click **Write**.
The files should now be fully recovered.

See "Check your disk with Norton Disk Doctor" on page 206.

23 Open Norton Disk Doctor and diagnose the affected drive to validate the corrections that you made.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- Online Service and Support
  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- PriorityCare telephone support
  This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:
http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Authorized Service Center
Postbus 1029
3600 BA Maarssen
The Netherlands

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

June 3, 2003

Glossary

access privileges	The types of operations that a user can perform on a system resource. For example, a user can have the ability to access a certain directory and open, modify, or delete its contents.
ActiveSync	The synchronization software for Microsoft Windows-based Pocket PCs.
ActiveX	A method of embedding interactive programs into Web pages. The programs, which are called controls, run when you view the page.
alert	A message that appears to signal that an error has occurred or that there is a task that requires immediate attention, such as a system crash or a Virus Alert.
alias	A shortcut icon that points to an original object such as a file, folder, or disk.
AppleTalk	A protocol that is used by some network devices such as printers and servers to communicate.
attack signature	A data pattern that is characteristic of an Internet attack. Intrusion Detection uses attack signatures to distinguish attacks from legitimate traffic.
beam	To transfer certain programs and data between two handheld devices using built-in infrared technology.

boot record	A sector at the start of a disk that describes the disk (sector size, cluster size, and so on). On startup disks, the boot record also has a program that loads the operating system.
bootable disk	A disk that can be used to start a computer.
cache	A location on your disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them.
cache file	A file that is used to improve the performance of Windows.
compressed file	A file whose content has been made smaller so that the resulting data occupies less physical space on the disk.
connection-based protocol	A protocol that requires a connection before information packets are transmitted.
connectionless protocol	A protocol that sends a transmission to a destination address on a network without establishing a connection.
cookie	A file that some Web servers put on your disk when you view pages from those servers. Cookies store preferences, create online shopping carts, and identify repeat visitors.
denial-of-service attack	A user or program that takes up all of the system resources by launching a multitude of requests, leaving no resources, and thereby denying service to other users.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that assigns a temporary IP address to each device on a network. DSL and cable routers use DHCP to allow multiple computers to share a single Internet connection.
dial-up	A connection in which a computer calls a server and operates as a local workstation on the network.

DNS (Domain Name System)

The naming system used on the Internet. DNS translates domain names (such as www.symantec.com) into IP addresses that computers understand (such as 206.204.212.71).

DNS server (Domain Name System server)

A computer that maps domain names to IP addresses. When you visit www.symantec.com, your computer contacts a DNS server that translates the domain name into an IP address (206.204.212.71).

domain

The common Internet address for a single company or organization (such as symantec.com). See also host name.

DOS window

A method of accessing the MS-DOS operating system to execute DOS programs through the Windows graphical environment.

download

To transfer a copy of a file or program from the Internet, a server, or computer system to another server or computer.

driver

Software instructions for interpreting commands for transfer to and from peripheral devices and a computer.

encryption

Encoding data in such a way that only a person with the correct password or cryptographic key can read it. This prevents unauthorized users from viewing or tampering with the data.

Ethernet

A common method of networking computers in a LAN (local area network). Ethernet cables, which look like oversized phone cables, carry data at 10M/100M/1G bps.

executable file

A file containing program code that can be run. Generally includes any file that is a program, extension, or system files whose names end with .bat, .exe, or .com.

extension	The three-letter ending on a file name that associates the file with an activity or program. Examples include .txt (text) and .exe (executable program).
FAT (file allocation table)	A system table (used primarily by DOS and Windows 9x/Me) that organizes the exact location of the files on the hard drive.
file type	A code that associates the file with a program or activity, often appearing as the file name extension, such as .txt or .jpeg.
Finder	The program that manages your Macintosh disk and file activity and display.
firewall rule	Parameters that define how a firewall reacts to specific data or network communications. A firewall rule usually contains a data pattern and an action to take if the pattern is found.
fragmented	When the data that makes up a file is stored in noncontiguous clusters across a disk. A fragmented file takes longer to read from the disk than an unfragmented file.
fragmented IP packet	An IP packet that has been split into parts. Packets are fragmented if they exceed a network's maximum packet size, but malicious users also fragment them to hide Internet attacks.
FTP (File Transfer Protocol)	An application protocol used for transferring files between computers over TCP/IP networks such as the Internet.
hidden attribute	A file attribute that makes files harder to access and more difficult to delete than other files. It also prevents them from appearing in a DOS or Windows directory list.
host name	The name by which most users refer to a Web site. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.

HotSync	The synchronization software for Palm OS handheld devices.
HTML (Hypertext Markup Language)	The language used to create Web pages.
ICMP (Internet Control Message Protocol)	An extension to the basic Internet Protocol (IP) that provides feedback about network problems.
IGMP (Internet Group Management Protocol)	An extension to the basic Internet Protocol (IP) that is used to broadcast multimedia over the Internet.
IMAP4 (Internet Message Access Protocol version 4)	One of the two most popular protocols for receiving email. IMAP makes messages available to read and manage without downloading them to your computer.
infrared (IR) port	A communication port on a handheld device for interfacing with an infrared-capable device. Infrared ports do not use cables.
IP (Internet Protocol)	The protocol that underlies most Internet traffic. IP determines how data flows from one computer to another. Computers on the Internet have IP addresses that uniquely identify them.
IP address (Internet Protocol address)	A numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually shown as four groups of numbers separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.
Java	A programming language used to create small programs called applets. Java applets can be used to create interactive content on Web pages.

JavaScript	A scripting language used to enhance Web pages. Most sites use JavaScript to add simple interactivity to pages, but some use it to open pop-up ads and reset visitors' homepages.
macro	A simple software program that can be started by a specific keystroke or a series of keystrokes. Macros can be used to automate repetitive tasks.
NAT (network addresstranslation)	A method of mapping private IP addresses to a single public IP address. NAT allows multiple computers to share a single public IP address. Most DSL and cable routers support NAT.
network address	The portion of an IP address that is shared by all computers on a network or subnet. For example, 10.0.1.1 and 10.0.1.8 are part of the network address 10.0.1.0.
NTFS (NTFS file system)	A system table (used primarily by Windows 2000/ XP) that organizes the exact location of all the files on the hard drive.
packet	The basic unit of data on the Internet. Along with the data, each packet includes a header that describes the packet's destination and how the data should be processed.
partition	A portion of a disk that is prepared and set aside by a special disk utility to function as a separate disk.
POP3 (Post Office Protocol version 3)	One of the two most popular protocols for receiving email. POP3 requires that you download messages to read them.
port	A connection between two computers. TCP/IP and UDP use ports to indicate the type of server program that should handle a connection. Each port is identified by a number.

port number	A number used to identify a particular Internet service. Internet packets include the port number to help recipient computers decide which program should handle the data.
PPP (Point-to-Point Protocol)	A protocol for communication between two computers using a dial-up connection. PPP provides error-checking features.
protocol	A set of rules governing the communication and transfer of data between computers. Examples of protocols include HTTP and FTP.
proxy	A computer or program that redirects incoming and outgoing traffic between computers or networks. Proxies are often used to protect computers and networks from outside threats.
registry	A category of data stored in the Windows registry that describes user preferences, hardware settings, and other configuration information. Registry data is accessed using registry keys.
removable media	Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, CDs, DVDs, and Zip disks.
router	A device that forwards information between computers and networks. Routers are used to manage the paths that data takes over a network. Many cable and DSL modems include routers.
script	A program, written in a scripting language such as VBScript or JavaScript, that consists of a set of instructions that can run without user interaction.
service	General term for the process of offering information access to other computers. Common services include Web service and FTP service. Computers offering services are called servers.

SSL (Secure Sockets Layer)	A protocol for secure online communication. Messages sent using SSL are encrypted to prevent unauthorized viewing. SSL is often used to protect financial information.
subnet	A local area network that is part of a larger intranet or the Internet.
subnet mask	A code, in the form of an IP address, that computers use to determine which part of an IP address identifies the subnet and which part identifies an individual computer on that subnet.
synchronize	The process by which a handheld device and computer compare files to ensure that they contain the same data.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Standard protocols used for most Internet communication. TCP establishes connections between computers and verifies that data is properly received. IP determines how the data is routed.
threat	A program with the potential to cause damage to a computer by destruction, disclosure, modification of data, or denial of service.
Trojan horse	A program containing malicious code that is disguised as or hiding in something benign, such as a game or utility.
UDP (User Datagram Protocol)	A protocol commonly used for streaming media. Unlike TCP, UDP does not establish a connection before sending data and it does not verify that the data is properly received.
virus definition	Virus information that an antivirus program uses to identify and alert you to the presence of a specific virus.

wildcard characters	Special characters (like *, $, and ?) that act as placeholders for one or more characters. Wildcards let you match several items with a single specification.
worm	A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.

Index